(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005年2月3日 (03.02.2005)

PCT

(10) 国際公開番号
WO 2005/011192 A1

(51) 国際特許分類[7]: H04L 9/32, 9/08

(21) 国際出願番号: PCT/JP2004/009944

(22) 国際出願日: 2004年7月12日 (12.07.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-273445 2003年7月11日 (11.07.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町二丁目３番１号 Tokyo (JP).

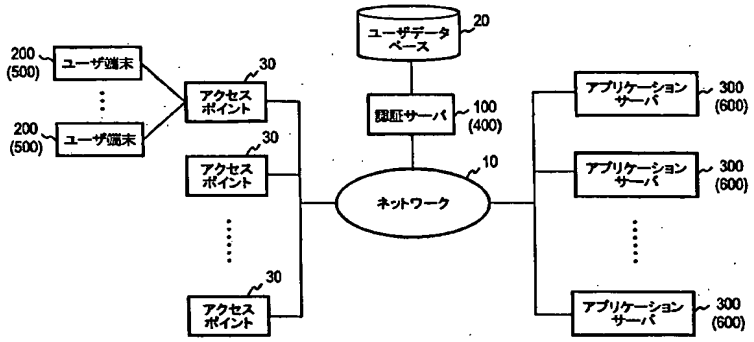
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 鶴岡 行雄 (TSURUOKA, Yukio) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 菊地 能直 (KIKUCHI, Yoshinao) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 水野 伸太郎 (MIZUNO, Shintaro) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 高橋 健司 (TAKAHASHI, Kenji) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 唐澤 圭 (KARASAWA, Kei) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP).

[続葉有]

(54) Title: AUTHENTICATION SYSTEM BASED ON ADDRESS, DEVICE THEREOF, AND PROGRAM

(54) 発明の名称: アドレスに基づく認証システム、その装置およびプログラム



200...USER TERMINAL
30...ACCESS POINT
20...USER DATABASE
100...AUTHENTICATION SERVER
10...NETWORK
300...APPLICATION SERVER

(57) Abstract: An address assigned to a user by an authentication server is used as an IP address of a packet transmitted from a user terminal. The IP address cannot be used for a bad purpose even when it is stolen. The authentication server (100) authenticates the user according to user authentication information transmitted from the user terminal. When the authentication is successful, an address is assigned to the user terminal and a ticket containing the address is issued and returned to the user terminal. The user terminal sets the address contained in the ticket as a transmission source address and transmits the ticket to an application server (300) to request to establish a session. After the server (300) checks whether the ticket is valid and stores the ticket if valid before establishing a session with the user terminal. By using this session, the user terminal transmits a packet requesting a service including the transmission source address to the server (300). The server (300) provides the service to the user if the transmission source address coincides with the address contained in the ticket stored.

(57) 要約: 認証サーバがユーザに割当てたアドレスをユーザ端末から送信するパケットのＩＰアドレスとし、そのＩＰアドレスが盗まれても悪用されない。認証サーバ１００はユーザ端末から送信されたユーザ認証情報に基いてユーザの認証を行い、認証が成功すると、ユーザ端末にアドレスを割当て、そのアドレスを含むチケットを発行してユーザ端末に返送する。ユーザ端末はチケットに含まれるアドレスを送信元アドレスに設定し、アプリケーションサーバ３０

[続葉有]

WO 2005/011192 A1

(74) 代理人: 草野 卓, 外(KUSANO, Takashi et al.); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿NSOビル4階 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

０にチケットを送信してセッションの確立を要求する。サーバ３００はチケットが正当なものと検証した後、チケットを記憶し、ユーザ端末とのセッションを確立する。ユーザ端末は、このセッションを用いて送信元アドレスを含むサービスを要求するサーバ３００に送信する。サーバ３００は、送信元アドレスと記憶したチケットに含まれるアドレスとが一致すれば、ユーザにサービスを提供する。

明 細 書

アドレスに基づく認証システム、その装置およびプログラム

技術分野

[0001] 本発明は、ユーザ端末が認証サーバによりユーザ認証を受け、その認証に基づき、アプリケーションサーバにサービスの提供を要求する認証システム、特に認証サーバにおいてユーザ認証に成功すると、ユーザ端末に送信元アドレスを割当て、ユーザが割当られた送信元アドレスを用いてアプリケーションサーバにサービスの提供を要求する認証システム、その装置およびプログラムに関する。

背景技術

[0002] 一般にユーザがインターネットのようなネットワークを通じてサーバからサービスの提供を受ける場合は、そのユーザの端末(ユーザ端末)とサーバとの間のセッションを確立し、そのセッションを通じてサーバに対し、サービス要求をする。サーバは提供したサービスに対する課金などの点からサービス提供に先立ち、ユーザ認証を行い、この認証に成功すると、確立したセッションを通じてサービスの提供をする。つまりサーバに対するサービスの要求が必要になるごとに、ユーザ認証が行われ、その時確立したセッションを通じてサービスの提供を受け、その際提供されるサービスが複数パケットによる場合でも同一セッションを通じてサービスの提供を受ける。

[0003] ところでユーザ認証を、各アプリケーションサーバがそれぞれサービス要求を受けるごとに行うには処理量が多くなるなどの点から、認証サーバがユーザ認証を行い、認証に成功するとそのユーザに対しIPアドレスを与え、ユーザはこのIPアドレスを送信元アドレスとしてサーバにサービスの提供を要求する方法が提案されている。

従来のネットワーク認証システムにおいては、このアドレスに基づく認証方法として例えば特許文献1に以下の方法が示されている。つまりユーザが接続サービスを利用する時に、接続認証サーバが、顧客情報とユーザID(ユーザを一意に識別する情報)との対応関係が予め格納されている個人情報データベースを参照してそのユーザを認証し、その認証が成功した場合に、接続の許可と共にIP(Internet Protocol)アドレスをユーザの端末に割当て、割当てたIPアドレスをユーザ端末に送信すると同

時にIPアドレスとユーザIDの関係を記憶装置に保持し、商取引サービス利用時にユーザ端末が、接続認証サーバから送信されたIPアドレスを用いて、インターネット上の販売サービス提供装置に購入する商品を申込み、販売サービス提供装置は、この商品の購入申込みパケットの送信元IPアドレスを取得し、このIPアドレスを接続認証サーバに送って問合せ、そのIPアドレスを元に記憶装置からユーザIDを取得し、更にその取得したユーザIDと対応する顧客情報を取得することにより、顧客の認証を行う。

特許文献1:特開2002−207929号公報

発明の開示

発明が解決しようとする課題

[0004] しかしながら、上述の従来の認証システムは、ユーザの接続認証時やサービス提供時に、第三者が、ユーザが使用しているIPアドレスをネットワーク上に送受されるパケットから盗み出し、盗み出したIPアドレスを用いて、商取引サービスを提供するサーバにアクセスすることにより、第三者によって成りすましが可能となってしまう課題がある。換言すれば、従来のアドレスに基づく認証システムでは、ユーザに割当てたアドレスの正当性を保証することができない。なお、正当なアドレスとは、ISP(internet service provider)などの機関がユーザまたはユーザの端末に対して正当な手順に従って割当てたアドレスである。

[0005] 本発明の目的は、このような従来の課題を解決するためになされたもので、ユーザに割当てたアドレスの正当性を保証することができるアドレスに基づく認証システム、その装置およびプログラムを提供することにある。

課題を解決するための手段

[0006] この発明によれば、ユーザを認証する認証サーバと、ユーザ認証情報を送信するユーザ端末と、ユーザ端末を介してユーザにサービスを提供するアプリケーションサーバとがネットワークを介して通信可能に接続された認証システムにおいて、

認証サーバは、

ユーザ端末からの認証要求として送信されたユーザ認証情報に基づいて認証手段によりユーザの認証を行い、そのユーザの認証が成功すると、ユーザ端末にアドレス

をアドレス割当手段により割当て、その割当てられたアドレスを含むチケットをチケット発行手段により発行し、その発行されたチケットをユーザ端末に送信し、

ユーザ端末は、

ユーザ認証情報を認証サーバへ送信し、認証サーバから送信されたチケットを受信し、そのチケットに含まれるアドレスを当該ユーザ端末から送信するパケットの送信元アドレスとして送信元アドレス設定手段により設定し、チケットを含むパケットをアプリケーションサーバに送信し、サービス要求手段によりサービスの要求を表すパケットをアプリケーションサーバに送信し、

アプリケーションサーバは、

ユーザ端末から送信されたチケットをチケット記憶手段に記憶し、ユーザ端末から送信されたサービスの要求を表すパケットの送信元アドレスがチケット記憶手段が記憶したチケットに含まれるアドレスと一致するか否かをアドレス判断手段により判断し、アドレスが一致すると判断されるとユーザにサービスを提供するパケットをサービス提供手段によりユーザ端末へ送信する。

発明の効果

[0007] この構成によれば、同一の認証サーバがユーザ認証を行い、かつアドレス割当を行っているため、正しいユーザにのみアドレスを割当てることができる。更に同一の認証サーバがアドレス割当とチケット発行を行っているため、チケットによりアドレスの正当性を保証できる。

ユーザ認証に基づきアドレスを発行しているので、アドレスの正当性が保証でき、しかもアプリケーションサーバへのチケットの送信は1回だけであり、このチケットに含まれるアドレスは、認証サーバにより正当なユーザがいま認証要求したユーザ端末に与えられたものであり、そのチケット内のアドレスが送信元アドレスとされているので、そのチケットの送信時に確立されたセッションを通じてユーザ端末から送信された各サービス要求パケットの送信元アドレスが記憶したチケット内のアドレスと一致すれば、そのパケットは認証されたユーザのパケットとみなせる。つまりセッション確立時に1回だけ送られたチケット内のアドレスを介して、サービス要求パケットの送信元アドレスが、認証されたユーザと結び付けられる。第三者がサービス要求パケットの送信元

アドレスを盗み、これを用いてアプリケーションサーバにサービス要求をしても、そのセッションでは記憶されたチケット内のアドレスと送信元アドレスとは不一致のものとなり、サービスの提供は行われない。

図面の簡単な説明

[0008] [図1]本発明の第1及び第2の実施の形態に係る認証システムのシステム構成例を示すブロック図である。

[図2]本発明の第1の実施の形態に係る認証サーバの機能構成例を示すブロック図である。

[図3]本発明の第1の実施の形態に係るユーザ端末の機能構成例を示すブロック図である。

[図4]本発明の第1の実施の形態に係るアプリケーションサーバの機能構成例を示すブロック図である。

[図5]本発明の第1の実施の形態で用いられるチケットの構成例を示す図である。

[図6]本発明の第1の実施の形態に用いられるチケットを含むパケットの構成例を示す図である。

[図7]本発明の第1の実施の形態に係る認証システムの処理手順の例を示すシーケンス図である。

[図8]本発明の第1の実施の形態に係る認証サーバの処理の流れの例を示すフローチャートである。

[図9]図9Aは本発明の第1の実施の形態に係るユーザ端末におけるユーザ認証時の処理の流れの例を示すフローチャート、図9Bはサービス要求時の処理の流れの例を示すフローチャートである。

[図10]本発明の第1の実施の形態に係るアプリケーションサーバの処理の流れの例を示すフローチャートである。

[図11]図11A及び図11Bはそれぞれ図2中の認証情報生成手段151のほかの機能構成例を示す図、図11Cは図4中の認証情報検証部320aの他の機能構成例を示す図である。

[図12]本発明の第2の実施の形態に係る認証サーバの機能構成例を示すブロック図

である。

[図13]本発明の第2の実施の形態に係るユーザ端末の機能構成例を示すブロック図である。

[図14]本発明の第2の実施の形態に係るアプリケーションサーバの機能構成例を示すブロック図である。

[図15]本発明の第2の実施の形態で用いるチケットの構成例を示す図である。

[図16]本発明の第2の実施の形態で用いる認証ヘッダが付加されたパケットの構成例を示す図である。

[図17]本発明の第2の実施の形態に係る認証システムの処理手順の例を示すシーケンス図である。

[図18]本発明の第2の実施の形態に係る認証サーバの処理の流れの例を示すフローチャートである。

[図19]図19Aは本発明の第2の実施の形態に係るユーザ端末におけるユーザ認証時の処理の流れの例を示すフローチャート、図19Bはサービス要求時の処理の流れの例を示すフローチャートである。

[図20]本発明の第2の実施の形態に係るアプリケーションサーバの処理の流れの例を示すフローチャートである。

[図21]図21Aは別の例の鍵情報を用いる場合の認証システムにおける処理手順の例を示すシーケンス図、図21Bは図12中の認証サーバに追加されるチャレンジ生成部の具体例を示すブロック図、図21Cは図13中の鍵情報生成部の他の具体例を示すブロック図、図21Dは図14中のチケット検証手段620内の一部変形例の具体例を示すブロック図である。

発明を実施するための最良の形態

[0009] 以下、図面を参照して本発明の実施の形態について詳細に説明する。以下の説明に応じて対応する部分には同一参照符号を付けて重畳説明を省略する。

(第1の実施の形態)システム構成

図1は、本発明の第1の実施の形態に係るアドレスに基づく認証システムのシステム構成図である。この発明のアドレスに基づく認証システムは、ユーザを認証する認証

サーバ100と、ユーザ認証情報を送信する複数のユーザ端末200を収容するアクセスポイント30と、ユーザにサービスを提供するパケットをユーザ端末200に送信する複数のアプリケーションサーバ300とが、ネットワーク10を介して通信可能に接続されて構成されている。

[0010] 認証サーバ100には、ユーザに関する情報(ユーザ認証データ)が格納されているユーザデータベース20が接続されている。ユーザは、ユーザ端末200を利用する利用者に限定されず、ユーザ端末200を直接操作しない利用者、例えば計算機がプログラムを実行することによりあたかも利用者がユーザ端末を利用しているかのように動作する場合のそのプログラム上の利用者であってもよい。また、このアドレスに基づく認証システムは、ユーザ端末200とアプリケーションサーバ300間の回線の安全性が物理的に確保される構成でもよい。この場合はユーザ端末200からアプリケーションサーバ300へ送信するパケットに対し改ざんの有無を確認できる処理をする必要がない。

[0011] ネットワーク10は、無線網、有線網を問わず、LAN(Local Area Network)またはインターネットなどによって構成されてもよい。アクセスポイント30は、地域毎に設置されてもよい。ユーザ端末200は、無線の通信が可能な携帯端末、若しくは、パソコンなどの端末でもよい。また、アプリケーションサーバ300は、映画およびスポーツ番組を含むコンテンツ配信サービス、電子商取引などのサービス、電子メール、IP電話、およびインスタントメッセージなどの通信サービス、またはWorld Wide Webなどの情報閲覧サービスを提供するサーバなどである。更にアプリケーションサーバ300は、別のネットワーク上のサービスへのアクセスを提供するゲートウェイサーバやファイアウォールなどであってもよい。

[0012] ユーザ端末200は、認証サーバ100がユーザを認証するために必要なユーザ認証情報を、アクセスポイント30を介して認証サーバ100に送信してユーザの認証を要求する。本実施形態においては、ユーザ認証情報には、ユーザ名およびパスワード、ユーザを認証するための鍵ペアに基づいて生成された情報、またはユーザの生体(例えば、指紋, 虹彩, 静脈パターン, 筆跡, 声紋等)を認証するための情報、などの公知の各種ユーザ認証方法に用いる情報のうち少なくとも1つが含まれる。なお、鍵

ペアは、公開鍵暗号技術に基づいた公開鍵と秘密鍵のペアである。

[0013] 認証サーバ100は、ユーザ端末200から送信されたユーザ認証情報に基づいてユーザデータベース20を参照してユーザの認証を行い、ユーザの認証が成功すると、ユーザと対応するユーザ識別子を割当て、その割当てたユーザ識別子と対応させるユーザ端末を一意に特定可能なアドレスを割当て、割当てたアドレスおよびユーザ識別子を含むチケットを発行し、発行されたチケットをユーザ端末200に送信する。

ユーザ端末200は、認証サーバ100から送信されたチケットに含まれるアドレスを、そのユーザ端末200から送信するパケットの送信元アドレスとし、アプリケーションサーバ300に、まずチケットを送信し、その後サービスを要求するパケット(以下サービス要求パケットという)を送信する。

[0014] アプリケーションサーバ300は、ユーザ端末200によって送信されたチケットを記憶し、記憶したチケットに含まれるアドレスとサービス要求パケットの送信元アドレスとが一致するか否かを判断し、アドレスが一致すると判断されるとユーザにサービスを提供するパケットをユーザ端末200へ送信する。

(第1の実施の形態)認証サーバ

図2は、本発明の第1の実施の形態で使用される認証サーバのブロック構成図である。認証サーバ100は、通信インターフェース101および制御処理手段102を備える。通信インターフェース101は、例えば、モデムまたはLANインターフェースなどによって構成され、ネットワーク10と接続される通信装置と通信可能にするものであれば如何なるものによって構成されてもよい。

[0015] 制御処理手段102は、プログラムを実行するCPU(Central Processing Unit)、およびプログラムを記憶するメモリなどを含む制御部102a、ユーザ認証情報受信手段110、認証手段120、ユーザ識別子割当手段130、アドレス割当手段140、チケット発行手段150、およびチケット送信手段160を有している。なお、これらの手段はそれぞれプログラムのモジュール、つまりハードウェアとして構成されることなく、プログラムの実行により機能するものでもよい。

先に述べたように認証サーバ100には、ユーザに関する情報が格納されているユーザデータベース20が接続されており、ユーザデータベース20は、ユーザを認証す

るときに使用する認証データ、およびユーザID(名前などそれ自体がユーザを一意に特定する情報)を含むユーザID登録データが格納されている。

[0016] ユーザ認証情報受信手段110は、ユーザ端末200から送信されたユーザ認証情報などを含む認証要求を通信インターフェース101を介して受信する。

認証手段120は、ユーザ認証情報受信手段110によって受信された認証要求のユーザ認証情報に基づいてユーザの認証を行う。認証手段120は、例えば、ユーザ認証情報とユーザデータベース20に格納されている認証データとの整合性を検証することによってユーザを認証する。

ユーザ識別子割当手段130は、ユーザの認証が成功すると、ユーザと対応するユーザ識別子ID_Uを、その認証要求に対し割当てる。ここで、ユーザ識別子は、ユーザ端末に割当てたアドレスに基づく認証システムにおいて一意の識別子である。あるいはユーザ識別子ID_Uは、認証サーバ内で一意な識別子をA、認証サーバのグローバルIPアドレスをBとしたとき、「A@B」などのように、グローバルに一意性を満たすよう拡張可能なものであってもよい。すなわち、想定されるユーザの集合において、ユーザ識別子はユーザに一意に対応づけられる。ただし、一人のユーザが同時に複数のユーザ識別子と対応してもよい。

[0017] ユーザ識別子割当手段130は、例えばユーザデータベース20に格納されているユーザID登録データからユーザIDを取得し、取得したユーザIDをユーザ識別子ID_Uとしてその認証要求に対し割当る。あるいは、ユーザ識別子割当手段130は、ユーザIDを取得したときに暗号化部140aで乱数を生成し、生成した乱数を取得したユーザIDに付加し、その(乱数+ユーザID)情報を、さらに認証サーバ100の識別子生成用秘密鍵で暗号化したものをユーザ識別子ID_Uとして割当ててもよい。このようにすれば、識別子生成用秘密鍵を知る者、例えば認証サーバ100のみがユーザ識別子ID_Uに基づいてユーザIDを知ることができるため、ユーザ識別子ID_Uがチケットに含められてアプリケーションサーバに送信されるが、ユーザのプライバシー保護を実現できる。また、ユーザ識別子割当手段130は、ユーザ認証情報からユーザ識別子ID_Uを割当てるようにしてもよいし、乱数、記号、シーケンス番号など、データベース等によりユーザIDに一意に対応付けることができるものをユーザ識別子ID_Uとしてもよ

い。

[0018] アドレス割当手段140は、ユーザ識別子割当手段130によって割当てたユーザ識別子ID_Uと対応させるユーザ端末にアドレスA_Uを割当てる。このアドレスA_Uは、IPアドレスの他、メールアドレス、SIP(Session Initiation Protocol)で扱われるURI(Uniform Resource Identifier)、またはIM(Instant Messaging)の相手名でもよい。

アドレス割当手段140におけるアドレス割当てについて、同一のアドレスを同時に複数のユーザ識別子と対応付けることがないとすれば、一つのアドレスに対して一意にユーザ識別子が対応し、したがって、ユーザも一意に対応付けられる。

[0019] 認証したユーザに割当てたユーザ識別子ID_Uと、割当てたアドレスA_Uとの対応がわかるように、その対応がもしくは対応付けの情報を含むチケットそのものが、例えば割当記憶部102bに、あるいはユーザデータベース20内のユーザ情報に、関連付けて記憶される。同一ユーザに対する割当てユーザ識別子ID_U、アドレスA_Uはその認証要求があるごとに変化してもよい、このため同一ユーザのチケットは、そのチケット発行日時などにより区別されるようにされる。また不要となったユーザ識別子ID_UおよびアドレスA_Uは適当な時期に削除される。このようにしてアプリケーションサーバ300からのユーザ識別子ID_Uに基づく、ユーザ情報の問合せや提供サービスに対する課金などに対応できるようにされている。

[0020] チケット発行手段150は、この例では認証情報生成手段151を含み、ユーザ識別子割当手段130によって割当てられたユーザ識別子ID_Uとアドレス割当手段140によって割当てられたアドレスA_Uとを含む仮のチケット(ID_U, A_U)を一時的に生成し、認証情報生成手段151によって仮のチケットに基づき認証情報IAを生成し、この認証情報IA、ユーザ識別子ID_U、アドレスA_Uを含むチケットCK1を発行する。

チケットCK1は例えば図5に示すように、ユーザ識別子、アドレス、認証情報の他に、チケットCK1を発行したときの日時を表わすタイムスタンプ、チケットの有効期間を表す情報、更に図5に示していないが、ユーザ端末200に割当てられた通信帯域幅を表す情報、およびユーザ端末200が収容されるアクセスポイント30に関する情報、例えば位置情報等などによって構成される。タイムスタンプを含ませる場合は、チケット発行手段150に時計部150aが設けられ、この時計部150aより出力するタイムスタ

ンプを利用する。チケットの有効期間を表す情報、およびユーザ端末200に割当てられた通信帯域幅を表す情報は、アクセスポイント30、認証サーバ100およびアプリケーションサーバ300などを運用する通信事業者やアプリケーションサービス事業者と、ユーザ端末200を使用するユーザとの契約によって予め決められるようにしてもよい。

[0021] 更に認証サーバ100を一意に識別する認証サーバ識別情報（例えばアドレスA_A）を例えば図5中に示すようにチケットCK1に加えても良い。あるいは先に述べたように、また図5中に示すとおり、認証サーバ100内で一意な識別子Aと認証サーバ100のグローバルIPアドレスBとを「A@B」と結合してユーザ識別子ID_Uとした場合、このBを認証サーバ識別情報として用いてもよい。

認証情報生成手段151は、例えばアプリケーションサーバ300との間で事前に共有する共有秘密鍵K_{CAS}と仮のチケット（ID_U, A_U）が一方向性ハッシュ関数演算器151aに入力され、仮のチケットに対し共有秘密鍵K_{CAS}を用いて一方向性ハッシュ関数を計算して認証子MACを生成し、これを認証情報IAとして出力する。

[0022] チケット送信手段160は、チケット発行手段150によって発行されたチケット51を通信インターフェース101を介してユーザ端末200に送信する。

（第1の実施の形態）ユーザ端末

図3は、本発明の第1の実施の形態で使用されるユーザ端末のブロック構成図である。ユーザ端末200は、通信インターフェース201および制御処理手段202を備える。通信インターフェース201は、例えば、有線もしくは無線のLANインターフェース、モデム、または携帯電話などの通信機器などによって構成され、アクセスポイント30を介してネットワーク10と接続される通信装置と通信可能にするものであれば如何なるものでもよい。

[0023] 制御処理手段202は、プログラムを実行するCPU、およびプログラムを記憶するメモリなどを含む制御部202a、認証要求手段203およびサービス要求手段230を有している。これらの手段は認証サーバ100と同様にプログラムのモジュール、つまりプログラムを実行することにより機能させてもよい。認証要求手段203は、ユーザ認証情報生成手段210、ユーザ認証情報送信手段220、およびチケット受信手段231を

有している。

ユーザ認証情報生成手段210は、ユーザ名およびパスワードを表す情報などを含むユーザ認証情報を生成する。ユーザ認証情報生成手段210は、例えば、キーボードなどの入力機器40からユーザ名およびパスワードが入力されると、その入力された情報に応じてユーザ認証情報を生成する。ユーザ名およびパスワードの他、ユーザ認証情報には、ユーザを認証するための鍵ペアに基づいて生成された情報、またはユーザの生体を認証するための情報などの公知のユーザ認証方法に用いられる、認証サーバ100がユーザを認証するために必要とする各種情報のうち少なくとも1つが用いられる。

[0024] ユーザ認証情報送信手段220は、ユーザ認証情報生成手段210によって生成されたユーザ認証情報を通信インターフェース201を介して認証サーバ100に送信して認証要求をする。

チケット受信手段231は、認証サーバ100から送信されたチケット(CK1)51を含むパケットを通信インターフェース201を介して受信し、受信したチケット51に含まれるアドレスA_Uを通信インターフェース201内、例えばレジスタ201aに送信元アドレスA_Sとして送信元アドレス設定手段231aにより設定登録する。なお、サービス要求手段230の送信元アドレス設定手段230aが受信したチケット51に含まれるアドレスを送信元アドレスA_Sとして通信インターフェース201内のレジスタ201aに設定登録するようにしてもよい。

[0025] サービス要求手段230は、セッション確立手段232を含み、アプリケーションサーバ300が提供するサービスを要求する。

セッション確立手段232は、ユーザが利用するサービスに応じてアプリケーションサーバ300とユーザ端末200との間にセッションを確立する。例えば、セッション確立手段232は、そのセッション確立処理におけるいずれかの過程で、通信インターフェース201を介してアプリケーションサーバ300に、チケット受信手段231によって受信されたチケット(CK1)51を送信してセッションを確立する。このセッション確立要求パケット52は例えば図6に示すように送信元アドレスA_Sを含むヘッダ部52hおよびチケット51を含むペイロード部52pによって構成される。

[0026] 例えば、セッション確立手段232は、パケット52を通信インターフェース201を介してアプリケーションサーバ300に送信する。通信インターフェース201は、チケット受信手段231の送信元アドレス設定手段231aによって登録されたアドレスA_Sをパケット52の送信元アドレスに設定し、設定したパケット52を送信する。サービス要求手段230は、確立したセッションを通してサービスの要求を表すパケット(サービス要求パケット)を、通信インターフェース201に登録されたアドレスを送信元アドレスA_Sとしてアプリケーションサーバ300に送信する。

[0027] (第1の実施の形態)アプリケーションサーバ

図4は、本発明の第1の実施の形態に使用されるアプリケーションサーバのブロック構成図である。アプリケーションサーバ300は、通信インターフェース301および制御処理手段302を備える。通信インターフェース301は、例えば、モデムまたはLANインターフェースなどによって構成され、ネットワーク10と接続される通信装置と通信可能にするものであれば如何なるものによって構成されてもよい。

制御処理手段302は、プログラムを処理するCPU、およびプログラムを記憶するメモリなどを含む制御部302a、サービス提供手段310、セッション確立手段311、およびチケット記憶手段330を有している。これらの手段は認証サーバ100と同様にプログラムのモジュールでもよい。

[0028] サービス提供手段310は、アドレス判断手段312を含み、ユーザ端末200から要求されるサービスを提供する。

セッション確立手段311は、チケット検証手段320を含み、ユーザ端末200とのセッションを確立する。セッションを確立する手順の中で、セッション確立手段311は、ユーザ端末200から送信されたチケット(CK1)51を含むパケット52を受信する。

チケット検証手段320は、パケット52に含まれるチケット(CK1)51が改ざんされているか否かを検証する。チケット検証手段320は例えば受信したチケット51内の認証情報IAを認証情報検証部320aで検証する。つまり認証情報IAが認証子MACであれば、認証サーバ100との間で事前に共有する共有秘密鍵K_{CSA}を用いて認証子検証部320aでチケット51が改ざんされているか否かを検証する。またチケット検証手段320は、チケット51に含まれるアドレスA_Uとパケット52の送信元アドレスA_Sとをアド

レス照合部320bで照合して、一致しなければ検証が失敗する。

[0029] 更にチケット検証手段320は、チケット(CK1)51に有効期間EPeが含まれている場合、時計部320dからの時刻情報により有効期間検証部320fにおいてチケット51が有効期間内か否かを検証するようにしてもよい。チケット検証手段320は、チケット(CK1)51に含まれるタイムスタンプTmsの値により、期間ごとに個別に用意された共有秘密鍵を選択して検証を行うようにしてもよい。チケット検証手段320は、チケット(CK1)51にタイムスタンプTmsが含まれている場合、タイムスタンプが表すチケット生成日時と時計部320dからの時刻情報より、チケット51が有効か否かを検証するようにしてもよい。あるいはチケット51に含まれるタイムスタンプおよび有効期間を表す情報に基づいてユーザの要求するサービスが、サービス提供手段310の提供有効期間内か否かを有効期間検証部320fで検証するようにしてもよい。

[0030] チケット検証手段320がチケット(CK1)51に含まれるアドレスA_Uとパケット52の送信元アドレスA_Sとを照合した結果が一致しており、チケットが正しいアドレスを持つユーザ端末から送信されていると判断すると、チケット記憶手段330に、そのチケット51を記憶する。しかしチケット検証手段320における他の検証や照合が一つでも成功しないとチケット51のチケット記憶部320aの記憶は阻止される。例えば各検出部320a, 320c, 320f、照合部320bの出力が記憶指令部320gに入力され、その入力の一つでも不成功を示せば、チケット51の記憶指令は発生しない。

[0031] アドレス判断手段312は、サービスの要求を表すパケットの送信元アドレスA_Sによりチケット記憶手段330を参照して、その送信元アドレスA_Sが対応する、チケット51に含まれるアドレスA_Uとが一致するか否かを検証する。サービス提供手段310は、チケット51に含まれるアドレスA_Uとパケットの送信元アドレスA_Sが一致すると、ユーザ端末200から要求されるサービスをユーザに提供するためのパケットをユーザ端末200に送信する。

サービス提供手段310は、チケット51に含まれるユーザ識別子ID_Uに基づき、必要に応じて、ユーザ情報を認証サーバ100に問い合わせてもよい。更にサービス提供手段310は、サービス提供に伴う課金などの情報を認証サーバ100を経由してユーザデータベース20に送信してもよい。これらの場合、図5中に示したようにチケットC

K1中に認証サーバ100の識別情報が含まれていれば、認証サーバが複数存在する場合は、これを直ちに特定でき、認証サーバ識別情報がアドレス(例えばアドレスA_A)の場合はそのアドレスを用いて直ちに認証サーバ100にアクセスすることができる。

[0032] (第1の実施の形態)認証システムの処理手順

本発明の第1の実施の形態に係るアドレスに基づく認証システムの処理手順について、図7を参照して説明する。

まず(1)ユーザの認証を認証サーバに要求する際に、ユーザ端末200はユーザ認証情報を生成し、このユーザ認証情報をアクセスポイント30を介して認証サーバ100へ送信する。

(2)この認証要求を受信した認証サーバ100はそのユーザ認証情報に基づいて、ユーザの認証を行う。認証サーバ100はユーザの認証が成功すると、ユーザにユーザ識別子ID_Uを割当て、更にそのユーザと対応づけられるユーザ端末200に対しアドレスA_Uを割当て、必要に応じて生成したアドレスA_Uに対する認証情報IA、タイムスタンプ、有効期間などを含むチケット51を発行して、(3)そのチケット51をユーザ端末200に送信する。

[0033] (4)チケット51を受信したユーザ端末200はチケット51のアドレスを送信元アドレスA_Sとして設定し、チケット51を含むパケット52をアプリケーションサーバ300へ送信して、アプリケーションサーバ300とのセッションの確立を要求する。

(5)パケット52を受信したアプリケーションサーバ300は認証情報によりチケットの正当性を検証し、検証に成功すればパケットの送信元アドレスA_Sとチケット51内のアドレスA_Uとを照合し、一致すればチケット51を記憶し、かつそのセッションを確立する。

[0034] (6)セッションが確立するとユーザ端末200はアプリケーションサーバ300に対して、サービス要求パケットを確立したセッションを通して送信する。

(7)サービス要求パケットを受信したアプリケーションサーバ300は、サービス要求パケットの送信元アドレスA_Sと記憶したチケット51に含まれるアドレスA_Uとが一致するか否かを判断し、アドレスが一致するとサービスをユーザに提供するためのパケットを

ユーザ端末200へ送信する。

(第1の実施の形態)認証サーバの処理

図8は、本発明の第1の実施の形態に使用する認証サーバ100の処理の流れを示すフローチャートである。

[0035] まず、ユーザ端末200から送信されたユーザ認証情報は、ユーザ認証情報受信手段110によって通信インターフェース101を介して受信され(S101)、ユーザ認証情報に基づいて認証手段120によってユーザの認証が行われ、ユーザの認証が成功すると、処理はS103へ進み、ユーザの認証が不成功なら、処理は終了する(S102)。

ユーザの認証が成功するとユーザ端末200にアドレスA_Uが割当てられる。この例ではユーザと対応するユーザ識別子ID_Uが、ユーザ識別子割当手段130によって割当てられ(S103)、このユーザ識別子ID_Uと対応づけるユーザ端末にアドレスA_Uが、アドレス割当手段140によって割当てられる(S104)。

[0036] 次に、この例ではユーザ識別子割当手段130によって割当てられたユーザ識別子ID_Uと、アドレス割当手段140によって割当てられたアドレスA_Uを含む仮のチケットが、チケット発行手段150によって一時的に生成され、認証子生成手段151によってアプリケーションサーバ300との間で事前に共有する共有秘密鍵を用いて仮のチケットに対し認証子MACが生成される(S105)。

次に、ユーザ識別子ID_U、アドレスA_U、認証子MACなどを含むチケット51が、チケット発行手段150によって発行され(S106)、このチケット51はチケット送信手段160によって通信インターフェース101を介してユーザ端末200に送信される(S107)。

[0037] (第1の実施の形態)ユーザ端末の処理

図9A及び図9Bは、本発明の第1の実施の形態に使用されるユーザ端末200の処理の流れを示すフローチャートである。

まず、図9Aに示すように、ユーザ名およびパスワードを表す情報などを含むユーザ認証情報が、ユーザ認証情報生成手段210によって生成され(S201)、このユーザ認証情報はユーザ認証情報送信手段220によって通信インターフェース201を介して認証サーバ100に送信される(S202)。

[0038] 認証サーバ100から送信されたチケット51は、チケット受信手段231によって受信される(S203)。

図9Bに示すように、チケット51が受信された後、アプリケーションサーバ300とのセッションが、セッション確立手段232によって確立される(S204)。アプリケーションサーバ300とのセッションが確立された後、サービスの要求を表すパケットが、サービス要求手段230によってセッションを通してアプリケーションサーバ300に送信される(S205)。

[0039] (第1の実施の形態)アプリケーションサーバの処理

図10は、本発明の第1の実施の形態に使用されるアプリケーションサーバ300の処理の流れを示すフローチャートである。

まず、ユーザ端末200とのセッションの確立が、セッション確立手段311によって開始され(S301)、パケット52に含まれるチケット51がアプリケーションサーバ300によって受信される。チケット51は、チケット検証手段320によって検証され、チケット51が正しいと検証されると、処理はS303へ進み、チケット51が改ざんされているなど正しくないと検証されると、処理は終了する(S302)。

[0040] チケット51が正しいと検証されると、セッションは、セッション確立手段311によって確立され、チケット51がチケット記憶手段330に記憶される(S303)。ユーザ端末200から送信されたサービスを要求するパケットが受信され、そのパケットの送信元アドレスA_Sと記憶したチケット51に含まれるアドレスA_Uとが一致するか否かがアドレス判断手段312により判断され(S304)、アドレスが一致すると判断されると、サービスが、サービス提供手段310によってユーザ端末200を介してユーザに提供されるためのパケットが送信される(S305)。送信元アドレスA_SとアドレスA_Uとが一致しなければ終了となる。

[0041] 以上説明したように、本発明の第1の実施の形態に係るアドレスに基づく認証システムは、ユーザ認証に基づきアドレスを発行しているので、正しいユーザ(ユーザ識別子)にそのアドレスを発行したことを保証できる。このような関係があり、認証サーバ100が、割当てたアドレスおよびユーザ識別子を含むチケット51を発行し、ユーザ端末200が、発行されたチケット51をアプリケーションサーバに送信し、アプリケーショ

ンサーバ300が、送信されたチケット51を検証すると共に記憶し、ユーザ端末200から送信されたサービス要求パケットの送信元アドレスと、記憶したチケット51に含まれるアドレスとを照合し、一致すれば、そのサービス要求パケットを、認証されたユーザのパケットとみなすことにより、アドレスに基づく認証が可能となる。

[0042] つまり、ユーザ認証に基づき認証サーバで発行されたチケットにより、ユーザ(識別子)とアドレスの対応が保証されていることから、サービス要求パケットの送信元アドレスA_Sと記憶したチケット内のアドレスA_Uとを照合することにより、そのパケットが認証されたユーザのものか否かを確認できる。

また、この実施形態ではアプリケーションサーバ300と認証サーバ100との間で事前に共有する共有秘密鍵を用いて生成される認証情報によってチケット51の正当性を検証するため、認証サーバ100によって発行されたチケット51、特にその内部のアドレスの正当性を保証することができる。

[0043] また、この実施形態では認証サーバ100がチケット51の有効期間を表す情報を含むチケット51を発行し、アプリケーションサーバ300が前記有効期間によってチケット51の有効性を検証するため、認証サーバ100の運営方針に従って有効期間を決定することができる。

(第1の実施の形態)変形

認証サーバ100において、ユーザ識別子割当手段130は必ずしも設けられなくてもよい。発行するチケット51の構成の1つとしてのユーザ識別子を省略してもよい。この場合はユーザ識別子割当手段130は省略され、また図8中に破線で示すようにステップS102で認証に成功すると直ちにステップS104に移る。しかしユーザ識別子を用いれば、チケット51自体でユーザ端末200に割当てたアドレスA_Uとユーザとが対応付けられ、従って例えばアプリケーションサーバ300からユーザ識別子を用いて、そのユーザ情報を認証サーバ100に問合せることができる。ユーザ識別子が省略されている場合はこの問合せをアドレスA_Uを用いて行い、認証サーバ100ではユーザ端末に割当てたアドレスA_UとそのユーザIDとの対応を記憶しておく必要がある。

[0044] 認証情報生成手段151で生成する認証情報IAは認証子MACに限らない。例えば図11Aに示すように、仮チケット(ID_U, A_U)を署名演算部151bに入力して、公開

鍵暗号技術に基づく認証サーバ100の秘密鍵K_{SA}を用いて仮チケット(ID_U, A_U)に対しディジタル署名演算を行って署名を生成し、これを認証情報IAとしてもよい。あるいは図11Bに示すように認証情報生成手段151に入力された仮チケット(ID_U, A_U)をアプリケーションサーバ300との共有秘密鍵K_{CAS}を用いて暗号化部151cで暗号化してその暗号化された仮チケットを認証情報IAとしてもよい。

[0045] 認証情報IAとして署名が用いられる場合、アプリケーションサーバ300内の認証情報検証部320aは図4中に括弧書きで示すように、認証子検証部の代りに署名検証部となり、認証情報IAとしての署名が認証サーバ100の公開鍵K_{PA}により署名検証処理される。またチケット51の全体が暗号化されて認証情報IAとされた場合は、認証情報検証部320aは図11Cに示すように認証情報IAが復号部320a1で認証サーバ100との共有秘密鍵K_{CAS}により復号され、その復号結果と、上記仮チケット(ID_U, A_U)との照合が照合部320a2で行われ、一致すれば検証に成功したとされる。

[0046] なお、チケット51の要素としてユーザ識別子を用いない場合は仮チケットはアドレスA_Uのみとなる。またチケット51の要素としてタイムスタンプなどを含む場合はこれらも仮チケットとして、仮チケットに対する認証情報IAを作成する。要はチケット51は認証情報IA以外の全ての要素を仮チケットとして認証情報IAを作成してもよい。

チケット51中の認証情報IAを省略してもよい。つまり図8中に破線で示すようにステップS104の後、直ちにステップS106へ移ってもよい。しかし認証情報IAを用いれば、アプリケーションサーバ300において、図10中に破線で示すようにステップS302におけるチケットに対する検証は、まず認証情報IAを検証して、仮チケットに対する改ざんが行われていないかを検証し(S302a)、チケットが改ざんされていなく、従ってチケット51中のアドレスA_Uが改ざんされていない正しいものであることが確認されると、送信元アドレスA_Sとチケット内のアドレスA_Uとの照合により、両アドレスが一致しているかが確認され(S302b)、一致していればステップS303へ移り、一致していなければ処理は終了する。

[0047] チケット51中の要素、タイムスタンプ、有効期間の一方あるいは双方とも省略してもよい。アプリケーションサーバ300においてユーザ端末200とのセッションが確立されるごとにそのユーザ端末200より受信したパケット中のチケットCK1を直ちにチケット

記憶手段330に記憶してもよい。つまり図4中のチケット検証手段320を省略し、図10中に破線31で示すように処理S301から直ちに処理S303へ移ってもよい。このようにしてもチケットCK1の送信は各セッションが確立されるごとに一度しかユーザ端末200からアプリケーションサーバ300へ送信されず、しかもユーザ端末200が新たにサービスが必要となるごとに認証サーバ100によりユーザ認証をしてもらい、従ってそのユーザ端末200に割当てられるアドレス(チケットCK1内のアドレス)が異なるものとなるから、第三者が送信元アドレスA_sを盗み、成りすましをすることは困難である。

[0048] 認証サーバ100にユーザデータベース20が必ずしも接続されていなくてもよい。例えばユーザ認証を公開鍵暗号技術を用いて行う場合は認証データを必要としない。しかしユーザ端末200から送信されたユーザの公開鍵証明書が信頼されるものであるかを確認するため、その公開鍵証明書を発行した公開鍵証明書発行機関に問合せ、正当なものであれば、その公開鍵証明書内のユーザ情報を、これで不足の場合は前記公開鍵証明書発行機関内のデータベースが対応ユーザに関する情報を取得する。

認証サーバ100は安全なネットワークで接続され、相互に信頼関係を持つサーバ群で構成してもよい。たとえば、認証専用サーバ、アドレス発行サーバ、チケット発行サーバなどが安全なネットワーク接続された構成でもよい。

[0049] (第2の実施の形態)認証システム構成

以下にこの発明の第2の実施の形態を、第1の実施の形態と違う部分を主に説明する。この第2の実施の形態においても、認証サーバとユーザ端末と、アプリケーションサーバとを備え、これらは機能的に第1の実施の形態のそれと異なる点をもっているが、システム構成は図1に示した第1の実施の形態と同様であるので、図1中に第2の実施の形態の参照番号を括弧書きで示す。認証サーバ400と、ユーザ端末500と、アプリケーションサーバ600とが、ネットワーク10を介して通信可能に接続されている。

[0050] 第2の実施の形態ではユーザ端末500は、認証サーバ400に対する認証要求の際に、ユーザ認証情報の他に鍵情報をも送信する。つまりユーザ端末500は鍵情報をもつものである。鍵情報は、ユーザ鍵ペアの公開鍵または端末鍵ペアの公開鍵、こ

れらの公開鍵を含む証明書、または公開鍵もしくは公開鍵を含む証明書に一方向性ハッシュ関数を適用して得られたハッシュ値などの、ユーザ又はユーザ端末の公開鍵に関連する情報を含む。

認証サーバ400は、ユーザ端末500からの認証要求に対し、ユーザの認証が成功して、チケットを発行する際に、ユーザ識別子およびアドレスの他に、この第2の実施の形態ではユーザ端末から送信された鍵情報をチケットに含める。

[0051] (第2の実施の形態)認証サーバ

図12は、本発明の第2の実施の形態に使用する認証サーバのブロック構成図である。認証サーバ400は、通信インターフェース101および制御処理手段402を備える。

制御処理手段402は、プログラムを処理するCPU(Central Processing Unit)、およびプログラムを記憶するメモリなどを含む制御部402a、ユーザ認証情報受信手段110、認証手段420、ユーザ識別子割当手段130、アドレス割当手段140、チケット発行手段450、およびチケット送信手段160を有している。なお、これらの手段はプログラムのモジュールでもよい。

[0052] 認証手段420は、ユーザ認証情報受信手段110によって受信されたユーザ認証情報に基づいてユーザの認証を行う。例えば、認証手段420は、ユーザ認証情報とユーザデータベース20に格納されている認証データとの整合性を認証情報照合部120aで検証してユーザを認証する。なお認証サーバは必要に応じて、ユーザ端末が鍵情報IKと関連する秘密鍵を保持しているか否かを確認するようにしてもよい。たとえば鍵情報IKに対応する公開鍵と対を成す秘密鍵の所有を確認するようにしてもよい。

チケット発行手段450は、認証情報生成手段151を含み、アドレス割当手段140によって割当てられたアドレスA_Uと、ユーザ識別子割当手段130によって割当られたユーザ識別子ID_Uと、ユーザ端末500からユーザ認証情報と共に送信された鍵情報と、認証情報生成手段151によって生成された認証情報IAとを含むチケットを発行する。このようにしてチケットは、ユーザ識別子と鍵情報を対応づける。すなわち、認証されたユーザと、鍵情報と関連する秘密鍵を保持するユーザ端末とを結びつけること

になる。チケットには、チケットを発行したときのタイムスタンプ、チケットの有効期間、ユーザ端末500に割当てられた通信帯域幅、およびユーザ端末500が収容されるアクセスポイント30に関する情報などを含めてもよい。このチケット53の例を図15に示す。チケット53は第1の実施の形態で用いたチケット51とは鍵情報を含む点で異なっている。

[0053] 認証サーバ400は認証要求を受けユーザ認証に成功すると、そのユーザにユーザ識別子を割当て、更にそのユーザ識別子と対応づけるユーザ端末にアドレスを割当てる。このアドレスがユーザ端末500で第1の実施の形態の場合と同様に送信元アドレスとして設定される。鍵情報はユーザ端末500の公開鍵と関連したものであるから、認証サーバ400は、ユーザとそのユーザが利用するユーザ端末500とを鍵情報により結びつけて(組として)ユーザ認証をしたことになり、かつその鍵情報をもつユーザ端末にアドレスが割当てられたことになる。

[0054] この第2の実施の形態によれば、ユーザ認証のためのユーザ鍵ペアとセッション確立用の端末鍵ペアを異ならせ、ユーザ鍵ペアを、ユーザ端末に接続した認証デバイスに保持させることにより、どの場所のユーザ端末でも、認証デバイスを接続することで、利用することができるようになる。なおユーザ認証方法として鍵ペアを利用しない方法を用いることもできる。

(第2の実施の形態)ユーザ端末

図13は、本発明の第2の実施の形態に使用するユーザ端末のブロック構成図である。ユーザ端末500は、通信インターフェース201および制御処理手段502を備える。制御処理手段502は、プログラムを処理するCPU、およびプログラムを記憶するメモリなどを含む制御部502a、認証要求手段503、およびサービス要求手段530を有している。なお、これらの手段はプログラムのモジュールでもよい。また、認証要求手段503は、ユーザ認証情報入力手段510、ユーザ認証情報送信手段220、およびチケット受信手段231を有している。

[0055] ユーザ認証情報入力手段510は、ユーザ認証情報などを認証デバイス41から入力させる。認証デバイス41に格納されたユーザ鍵ペアのうち秘密鍵は、認証デバイス41から持ち出せない。また、認証デバイス41は、ICカード、USB(Universal Serial

Bus)キーなどを含むハードウエア認証トークン、または生体認証装置などである。あるいは入力機器40からパスワード・ユーザ名をユーザ認証情報生成手段210に入力してユーザ認証情報を生成してもよい。なお、簡易的な方法として認証デバイス41がユーザ端末500に接続されない場合は、ユーザ鍵ペアの代用として鍵格納部502bに格納された端末鍵ペアを用いてユーザ認証情報を生成してもよい。

[0056] また鍵情報生成部503aは鍵格納部502bからユーザ端末500の公開鍵を入力して鍵情報を生成する。鍵情報生成部503aは入力された公開鍵をそのまま鍵情報として出力してもよい。ユーザ認証情報送信手段220はユーザ認証情報のみならず鍵情報も認証サーバ400に送信して認証要求をする。

サービス要求手段530は、セッション確立手段532およびパケット暗号処理手段533を含み、アプリケーションサーバ600が提供するサービスを要求する。セッション確立手段532は、IKE(Internet Key Exchange)などに準拠して、チケット53に含まれる鍵情報と関連する公開鍵と対をなす秘密鍵K_{SS}とアプリケーションサーバ600の公開鍵K_{PS}とからアプリケーションサーバ600と互いに共有する秘密鍵をセッション秘密鍵K_{CUS}として、セッション秘密鍵生成部532aで生成する。

[0057] パケット暗号処理手段533は、アプリケーションサーバ600とセッション秘密鍵が共有された後、つまりアプリケーションサーバ600でもユーザ端末500と互いに共有する秘密鍵をセッション秘密鍵として生成した後、IPsec(SECurity architecture for the Internet Protocol)またはTLS(Transport Layer Security)などに準拠して、セッション確立手段532によってアプリケーションサーバ600との間で共有されたセッション秘密鍵を用いて、送信するパケットの情報に対する認証ヘッダを認証ヘッダ生成部533aで計算し、この認証ヘッダAHを、送信するパケットに付加する。認証ヘッダ生成部533aはパケットを改ざんしたか否かがわかるように、パケットに対しセッション秘密鍵を用いて一方向性ハッシュ関数を計算して認証ヘッダを生成する。また、パケット暗号処理手段533は図13中に括弧書きで示すように、IPsecまたはTLSなどに準拠してパケットを暗号化部533a′で暗号化してもよい。あるいはパケット54に認証ヘッダAHを付けた上でパケットに対して暗号化部533a′で暗号化してもよい。これら認証ヘッダAHの付加処理、パケットの暗号化処理を総称して、パケット暗号処理とい

い、またその処理を行う構成をパケット暗号処理手段という。

[0058] 図16にパケット暗号処理手段533により生成したパケット54の構成例を示す。図6に示したパケット52とは、ヘッダ部54hに認証ヘッダが付加され、ペイロード部54p中のチケット53に鍵情報が付加されている点が異なる。なおパケットが暗号化部532bにより暗号化されると共に、認証ヘッダAHを付けてもよい。

(第2の実施の形態)アプリケーションサーバ

図14は、本発明の第2の実施の形態に使用するアプリケーションサーバのブロック構成図である。アプリケーションサーバ600は、通信インターフェース301および制御処理手段602を備える。制御処理手段602は、プログラムを処理するCPUおよびプログラムを記憶するメモリなどを含む制御部602a、サービス提供手段610、セッション確立手段611、およびチケット記憶手段330を有している。なお、これらの手段はプログラムのモジュールでもよい。

[0059] サービス提供手段610は、アドレス判断手段312、およびパケット認証手段612を備え、ユーザ端末500から要求されるサービスを提供する。

セッション確立手段611はチケット検証手段620を含み、ユーザ端末500とのセッションを確立する。セッションを確立する手順の中で、IKEなどに準拠してセッション秘密鍵をユーザ端末500と互いに共有する。つまりセッション確立手段611は、鍵格納部602b内のアプリケーションサーバ600の秘密鍵K_{SA}とユーザ端末500の公開鍵K_{PU}とを用いてユーザ端末500と互いに共有する秘密鍵をセッション秘密鍵K_{CUS}としてセッション秘密鍵生成部611aにより生成する。

[0060] パケット認証手段612は、ユーザ端末500とセッション秘密鍵が共有された後、受信したパケット54に付加された認証ヘッダAHをセッション秘密鍵K_{CUS}を用いて検証する。パケット認証手段612は、パケット54に付加された認証ヘッダの検証結果が正常であればパケット54内のチケット(CK2)53をチケット検証手段620に出力する。受信したパケット54がユーザ端末500で暗号化されている場合は、パケット認証手段612ではなく、括弧書きで示すようにパケット復号手段612′が用いられ、パケット54がセッション秘密鍵K_{CUS}で復号され、正しく復号されると、つまりパケット54が改ざんされていなければ、復号されたパケット54をチケット検証手段620へ出力する。前記認

証ヘッダAHの認証処理、パケット54の復号処理を総称してパケット検証といい、その検証を行う構成をパケット検証手段という。

[0061] チケット検証手段620は、パケット認証手段612によって出力されたチケット53の正当性を検証する。例えば、チケット検証手段620は、鍵照合部620aでチケット53に含まれる鍵情報IKとセッション秘密鍵K_{CUS}の共有に用いたユーザ側の公開鍵とを照合し、その整合性がとれ、かつこの例ではまたチケット53に含まれるアドレスA_Uとパケット54の送信元アドレスA_Sとをアドレス照合部320bで照合し一致した場合、これを記憶指令部620cが検出してチケット記憶手段330に、チケット(CK2)53を記憶する。ユーザ端末500とのセッションが確立され、前記チケット(CK2)53がチケット記憶手段330に記憶された後、そのセッションを通じてユーザ端末500からサービス要求パケットを受信すると、サービス提供手段610は、パケット認証手段612(又はパケット復号手段612′)によりIPsecまたはTLS等に準拠してパケット54が改ざんされてないことが確認された(又は復号された)パケット54の送信元アドレスとチケット記憶手段330に記憶されている対応チケット(CK2)53に含まれるアドレスとが一致するとアドレス判断手段312によって判断されると、ユーザ端末500から要求されるサービスをユーザに提供するためのパケットをユーザ端末500の前記セッションを通じて送信する。なお、チケット検証手段620は必要に応じて認証情報検証部320aなど、第1実施形態中のアプリケーションサーバ300と同様、図4中のチケット検証手段320に設けることができる各種検証部を設けてもよい。

[0062] (第2の実施の形態)認証システムの処理手順

以下、本発明の第2の実施の形態に係るアドレスに基づく認証システムの処理手順を図17を参照して説明する。

まず、(1)ユーザ端末500でユーザ認証情報および鍵情報IKを生成し、アクセスポイント30を介して認証サーバ400に認証要求を送信する。

(2)認証サーバ400は認証要求を受信するとユーザ認証情報に基づいて、ユーザの認証を行い、ユーザの認証に成功すると、ユーザ識別子ID_Uの割当て、ID_Uと対応づけるユーザ端末にアドレスA_Uの割当てを行い、更に必要に応じて認証情報を生成し、ユーザ識別子ID_U、アドレスA_Uおよび鍵情報IKなどを含むチケット53を発行し、

(3)そのチケットをユーザ端末500に送信する。

[0063] (4)ユーザ端末500は受信したチケット中のアドレスA_Uを送信元アドレスとし、

(5)ユーザ端末500は自己の秘密鍵K_{SU}とアプリケーションサーバ600の公開鍵K_{PS}を用いてIKEなどの鍵交換手順に準拠して、アプリケーションサーバ600と共有するセッション秘密鍵K_{CUS}を計算する。このセッション秘密鍵K_{CUS}を用いて、アプリケーションサーバ600に送信するパケットについて認証ヘッダAHを生成し、これをパケットに付加するようにする。さらにセッション確立の過程において、認証ヘッダおよびチケットを含むパケットをアプリケーションサーバ600に送信する。以上の手順によりアプリケーションサーバ600に対してセッションの確立を要求をする。

[0064] (6)アプリケーションサーバ600は、セッション確立の過程において、自己の秘密鍵K_{SS}とユーザ端末の公開鍵K_{PU}を用いてセッション秘密鍵K_{CUS}を計算し、このセッション秘密鍵K_{CUS}を用いてパケットに付加された認証ヘッダAHを検証し、更に必要に応じてセッション確立過程中に受信したチケット(CK2)53中の認証情報IAを認証サーバ400との共有秘密鍵K_{CAS}で検証する。また受信されたチケット53に含まれる鍵情報が、セッション秘密鍵K_{CUS}の計算に用いられたユーザ側の公開鍵(ユーザ公開鍵もしくは端末公開鍵)K_{PU}と対応するか否かを検証し、受信したパケット54の送信元アドレスA_Sと、チケット(CK2)53に含まれるアドレスA_Uとを照合し、これらが全て成功すればチケット(CK2)53を記憶し、セッションを確立する。

[0065] (7)ユーザ端末500は送信元アドレスA_Sを保護するためセッション秘密鍵K_{CUS}を用いて暗号化処理または認証ヘッダ付加処理のうち少なくとも1つを施し、サービスの要求を表すパケットをアプリケーションサーバ600にその確立されたセッションを通じて送信する。

(8)アプリケーションサーバ600ではサービス要求パケットをセッション秘密鍵K_{CUS}で復号し、または認証ヘッダを検証し、記憶したチケット53に含まれるアドレスと、サービス要求を表すパケットの送信元アドレスA_Sとが一致するか否かを判断し、アドレスが一致すれば、サービスをユーザに提供するためのパケットをユーザ端末500へ送信する。

[0066] (第2の実施の形態)認証サーバの処理

図18は、本発明の第2の実施の形態に使用する認証サーバの処理の流れを示すフローチャートである。

ユーザ端末500から認証要求が受信されると(S101)、ユーザ認証情報に基づいて認証手段120によってユーザの認証が行われ、ユーザの認証が成功すれば、処理はS103へ進み、ユーザの認証が失敗すれば処理は終了する(S102)。アドレスA_U、ユーザ識別子ID_U、鍵情報IKを含むチケット53は、チケット発行手段450によって発行される(S402)。その他の処理は第1の実施の形態の認証サーバの処理手順と同様である。

[0067] (第2の実施の形態)ユーザ端末の処理

図19は、本発明の第2の実施の形態に使用するユーザ端末の処理の流れを示すフローチャートである。

図19Aに示すユーザ認証要求処理ではユーザ認証情報と鍵情報IKは、ユーザ認証情報入力手段510によって入力され(S501)、ユーザ認証情報送信手段220によって通信インターフェース201を介して認証サーバ400に送信される(S202)。認証サーバ400から送信されたチケット(CK2)53は、チケット受信手段231によって受信される(S203)。

[0068] その後の図19Bに示すアプリケーションサーバ600とのセッションの確立処理では、セッション確立手段532によって開始され、セッション秘密鍵が、ユーザ端末500とアプリケーションサーバ600との間で共有される。ここで、チケット53を含むパケット54は、パケット処理手段533によって認証ヘッダ付加処理および／又は暗号化処理が施され、アプリケーションサーバ600に送信される(S502)。

次に、アプリケーションサーバ600とのセッションが確立された後、サービスの要求を表すパケットは、サービス要求手段530によってその確立されたセッションを通してアプリケーションサーバ600に送信されることによって、サービスがアプリケーションサーバ600に要求される(S205)。

[0069] (第2の実施の形態)アプリケーションサーバの処理

図20は、本発明の第2の実施の形態に使用するアプリケーションサーバの処理の流れを示すフローチャートである。

まず、ユーザ端末500とのセッションの確立は、セッション確立手段611によって開始され、IKEなどの鍵交換手順に準拠して互いの自秘密鍵と相手公開鍵から計算して得られたセッション秘密鍵が、ユーザ端末500とアプリケーションサーバ600との間で共有される(S601)。ここで、ユーザ端末500によって送信されたチケット53を含むパケット54が、アプリケーションサーバ600によって受信される。

[0070] 受信されたパケット54に付加された認証ヘッダは、パケット認証手段612によって、セッション秘密鍵を用いて検証され、パケット54が改ざんされていない正しいものと検証された場合、処理はS603に進み、パケット54が改ざんされているなど正しくないと検証された場合、処理は終了する(S602)。なおパケット54が暗号化されている場合はパケット復号手段612′でセッション秘密鍵を用いて復号し、復号が正しく行われると処理はS603に進む。

チケット53の正当性が検証され、つまり少くともチケット53に含まれる鍵情報と、セッション秘密鍵の共有に用いたユーザ側の公開鍵との整合性が検証され、パケット54の送信元アドレスA_Sとチケットに含まれるアドレスA_Uが一致している場合には(S603)、チケット53は正しいものとして、チケット記憶手段330によって記憶される(S303)。

[0071] セッションが確立された後、ユーザ端末500から送信されたサービスを要求するパケットに対しパケットが改ざんされていない正しいものかが、パケット検証手段で検証され(S604)、正しければそのパケットの送信元アドレスは、記憶したチケット53に含まれるアドレスと一致するか否かが判断され、アドレスが一致すると判断されると(S304)、サービス提供手段610によってユーザ端末500を介してユーザにサービスが提供される(S305)。

なお、ユーザ端末500がチケット53を含むパケット54をアプリケーションサーバ600に送信するタイミングは、IKEなどの鍵交換手順の完了前でもよい。この場合には、鍵交換手順に先立って、ユーザ端末500から送られたチケット53を、チケット検証手段620により検証を行うことで、鍵交換手順を実行するか否かを事前に判断することができる。すなわち、チケットを持たないユーザ端末からの不正なサービス要求に対する処理を初期の段階で遮断できる利点が生じる。ただしチケット53を含むパケット5

4の送信が、ユーザ端末500とアプリケーションサーバ600間でセッション秘密鍵を共有する以前であり、パケット検証手段を機能させることができないから、パケット54に対する改ざんの検出が出来ず、チケットの差し替えなどの不正の可能性が生じる。しかし、チケット53に含まれる認証情報により、チケット検証手段620でチケット53自身の改ざんが検出できること、さらには鍵交換が終了した時点で、鍵交換に用いたユーザ側の公開鍵と、チケット53に含まれた鍵情報との整合性を検証することによりチケットが正しいユーザ端末から送られていることが確認できる。つまり鍵交換手順の完了前(直前もしくは手順中)にユーザ端末500からアプリケーションサーバ600へチケット53を送った場合においても最終的には安全性が保持できる。

[0072] 以上説明したように、本発明の第2の実施の形態に係るアドレスに基づく認証システムは、認証サーバが、ユーザ端末を介して行うユーザ認証の結果に基づき、ユーザ識別子、アドレス、鍵情報の対応付けを保証するチケットをユーザ端末に送信し、ユーザ端末が、アプリケーションサーバにチケットを送信すると共にセッション秘密鍵を共有することでセッションを確立し、そのセッションを通してアプリケーションサーバにサービスを要求し、アプリケーションサーバは、受信したチケットの正当性を確認した後チケットを記憶し、受信したサービス要求のパケットの送信元アドレスと、記憶されたチケットに含まれるアドレスとを照合することでサービス要求を検証し、正しく検証された場合にサービスを提供するものである。

[0073] とくに、ユーザ端末500がアプリケーションサーバ600にパケットを送信する際に、セッション秘密鍵を用いて計算された認証ヘッダ等の改ざん検出のための情報をパケットに付加して送信し、アプリケーションサーバ600が、ユーザ端末500から送信されたパケットに対して改ざんされていないことを確認しているため、セッションを通して、ユーザ端末500からアプリケーションサーバ600へ送信されるパケット54に改ざんがないことを保証できる。すなわち、パケットに含まれる送信元アドレスに改ざんがないことが保証される。

[0074] また、前記例ではアプリケーションサーバにおいて、セッションを確立する際にユーザ端末から受信した情報、例えばユーザ側の公開鍵と、チケットに含まれる鍵情報との整合性を検証するため、確立したセッションとチケットとを関連付けることができる。

また、チケットは認証サーバにおいて、ユーザ端末を介したユーザ認証に基づいて発行され、ユーザ識別子とアドレスと鍵情報の関連付けを保証しているため、鍵情報と関連する鍵を持つユーザ端末と、ユーザ識別子により特定されるユーザとの対応付けが保証されている。したがって、確立したセッションとチケットにより、送信元アドレスとユーザの対応付けが保証される。

[0075] さらに、チケットは前記のとおりユーザ認証に基づいて発行されるため、チケットに含まれるアドレスの正当性を保証できる。また前記の通り、アプリケーションサーバに記憶されたチケットに含まれるアドレスとパケットの送信元アドレスを照合すること、パケットの送信元アドレスは確立したセッションにおいて改ざんがないことが保証されていることにより、パケットの送信元アドレスの正当性が保証される。結果として、パケットの送信元アドレスの正当性、送信元アドレスとユーザの対応付けが保証されることから、アドレスに基づく認証が可能となる。

[0076] なお、チケットによりアドレスの正当性の保証、即ち正しく認証されたユーザに正しい手順で払い出されたアドレスであることの保証、が可能となるのは、ユーザを認証する機能とアドレスを発行する機能、それらの関連付けを保証するチケット生成機能が、同一の認証サーバにより実現されているためである。また、チケットによりユーザと端末の対応付けの保証が可能となるのは、ユーザ端末を介したユーザ認証と同時に、ユーザ端末から認証サーバに鍵情報を送信する手順およびそのための構成により、ユーザと端末の関連付けを行っているためである。

[0077] なお、ユーザと端末とアドレスの対応付けは、鍵情報に関連する秘密鍵を端末から消去することで無効化できる。これは秘密鍵がなければ鍵交換ができず、また、異なる鍵を用いれば、チケットに含まれる鍵情報と整合しないため，いずれの場合もセッションの確立が成功しないためである。

（第2の実施の形態）変形

第2の実施の形態は鍵情報IKを利用した処理に関連する部分が第1の実施の形態と異なっている。従って第1の実施の形態においてその変形の項で説明した変形は、第2の実施の形態においても同様に可能である。

[0078] アプリケーションサーバ600で、アドレス照合部320bを省略して鍵照合部620aで

整合が取れることが確認できると、そのチケットCK2をチケット記憶手段330に記憶するようにしてもよい。

鍵情報IKとしてはユーザ端末の公開鍵と関連した情報に限らない。例えばユーザ端末500とアプリケーションサーバ600間で事前に認証用共有秘密鍵K_{US}を共有する場合には、その認証用共有秘密鍵K_{US}の所有を証明できる情報であってもよい。例えば図21Aのシーケンス図に示されるように、認証サーバ400においてユーザ認証に成功するとチャレンジ生成部460(図21B)でチャレンジbを生成してユーザ端末500に送信する。

[0079] ユーザ端末500は、認証要求手段503内の鍵情報生成部503b′ (図21C)を用いて、受け取ったbに対するレスポンスとして、bと認証用共有秘密鍵K_{us}を入力とした一方向性ハッシュ関数hの値r＝h(K_{US}, b)を計算し、チャレンジbとレスポンスrの組を鍵情報IK＝{b、r}として生成する。そして鍵情報IKが認証サーバ400に送信される。なおチャレンジbとしては、認証サーバ500から明示的に送信される値の代わりに、レスポンスを生成する時刻(タイムスタンプ)やセッション中のシーケンス番号などの暗黙のチャレンジを用いてもよく、この場合はチャレンジの送受信を省略できる。

[0080] 認証サーバ400では、受信した鍵情報IKに含まれるチャレンジbの正当性を確認し、正しく確認できたとき鍵情報IKを含むチケットCK2を発行する。なお、チャレンジの正当性はチャレンジbが明示的なもの、もしくはユーザ端末500と認証サーバ400の間のセッションに依存して一意に定まるものであれば、その一致を確認し、チャレンジbがレスポンスrを計算した時刻t1であるなど、暗黙のチャレンジであれば、t1とチケット発行時刻t2の差が許容範囲d内である(すなわちt2−t1≦d)などの条件によりその正当性を確認する。なお、共有秘密鍵を用いてチャレンジとレスポンスにより行う認証は公知技術であるため、より詳細な説明は省略する。

[0081] チケットCK2を受信したユーザ端末500は、サービス要求のためのセッションを確立する際に、前述したように、チケットCK2をアプリケーションサーバ600に送信する。

アプリケーションサーバ600では、チケット検証手段620内の端末認証部620d(図21D)により鍵情報IK＝{b、r}を入力し、共有秘密鍵K_{us}を用いてチャレンジbに対す

るハッシュ値(K_{US}, b)が再計算され、このハッシュ値と鍵情報IK内のレスポンスrとが一致するか否かが照合判定部で照合される。照合の結果が一致すれば端末認証部620dの照合判定部より記憶指令部620c(図14)に対して、記憶許可を示す指令が出力され、チケットが記憶される。

[0082] なおアプリケーションサーバ600の端末認証部620d(図21d)は、図21A中に破線で示すように、ユーザ端末500との間のセッションを確立する過程において付加的なチャレンジb′をユーザ端末に送信し、対応するレスポンスr′=h(Kus, b′)をユーザ端末500から受信し、r′の正当性の確認を行ってもよい。(この場合においてもb′を暗黙のチャレンジに置き換えてもよい。)

以上の手順により、アプリケーションサーバ600は、鍵情報IKに基づいて、セッション依存情報であるところのチャレンジb(b′)に対するレスポンスr(r′)が正しいものであることを確認することにより、ユーザ端末500がユーザ認証時(加えてサービス要求時)に共有秘密鍵K_{US}を保持していたことを認めることができる。

[0083] さらに、チケットCK2はユーザ認証に基づき発行されたのもであるから、鍵情報IKと、アドレスA_U、ユーザ識別子ID_Uの対応づけが保証され、したがって、鍵情報が指し示す共有秘密鍵K_{US}を持つユーザ端末に、アドレスA_Uが払い出されたことを保証できる。また、そのアドレスA_Uを送信元として行われたサービス要求が、認証されたユーザのものであることを保証できる。さらには認証されたユーザのID、名前、住所などと関連付けることができる。

更に鍵情報IKとしては最初の例のようにユーザ端末の公開鍵K_{PU}と関連した情報でもよく、ユーザ端末500とアプリケーションサーバ600との認証用共有秘密鍵を保持していることを証明する情報でもよいということは、要はユーザ端末500が、ユーザ端末500を、一般に、又はサービスを要求されたアプリケーションサーバが一意に識別できる秘密鍵つまり、前者でユーザ端末の鍵ペアの秘密鍵K_{SU}、後者では認証用共有秘密鍵K_{US}などの秘密鍵を保持していることをアプリケーションサーバ600が鍵情報IKに基づき検証することができる鍵情報IKであればよい。

[0084] 図2及び図12に示した各認証サーバ、図3及び図13に示した各ユーザ端末、図4及び図14に示した各アプリケーションサーバはいれずれもコンピュータに機能させて

もよい。例えばコンピュータに、図2に示した認証サーバとして機能させるための認証サーバプログラムを、CD−ROM、磁気ディスク、半導体記憶媒体などの記録媒体からインストールし、あるいは通信回線を有してダウンロードし、その認証サーバプログラムを実行させればよい。その他のものについても同様である。

請求の範囲

[1] ユーザを認証する認証サーバと、ユーザ認証情報を送信するユーザ端末と、ユーザ端末を介してユーザにサービスを提供するアプリケーションサーバとがネットワークを介して通信可能に接続された認証システムにおいて、

認証サーバは、

ユーザ端末からの認証要求として送信されたユーザ認証情報に基づいて、ユーザの認証を行う認証手段と、

ユーザの認証が成功すると、上記ユーザ端末にアドレスを割当てるアドレス割当手段と、

アドレス割当手段によって割当てられたアドレスを含むチケットを発行するチケット発行手段と、

チケット発行手段によって発行されたチケットを上記ユーザ端末に送信するチケット送信手段を備え、

ユーザ端末は、

ユーザ認証情報を認証サーバへ送信して認証要求するユーザ認証情報送信手段と、

認証サーバから送信されたチケットを受信するチケット受信手段と、

チケットに含まれるアドレスを当該ユーザ端末から送信するパケットの送信元アドレスとして設定する手段と、

チケットを含むパケットをアプリケーションサーバに送信し、セッションを確立する手段と、

サービスの要求を表すパケット(以下サービス要求パケットという)をアプリケーションサーバに送信するサービス要求手段を備え、

アプリケーションサーバは、

ユーザ端末から送信されたチケットを記憶するチケット記憶手段と、

チケット記憶手段が記憶したチケットに含まれるアドレスと、上記セッションを介してユーザ端末から送信されたサービスの要求を表すパケットの送信元アドレスとが一致するか否かを判断するアドレス判断手段と、

アドレス判断手段によってアドレスが一致すると判断されると、ユーザにサービスを提供するパケットを上記ユーザ端末へ送信するサービス提供手段を備えたことを特徴とするアドレスに基づく認証システム。

[2] 請求の範囲1の認証システムにおいて、

上記ユーザ端末はそのユーザ端末の秘密鍵と関連した鍵情報をもち、

上記ユーザ認証情報送信手段は上記鍵情報をもユーザ認証情報と共に送信する手段であり、

上記チケット発行手段は、ユーザ端末から送信された鍵情報も含むチケットを発行する手段であり、

ユーザ端末は、

当該ユーザ端末の秘密鍵とアプリケーションサーバの公開鍵からアプリケーションサーバと共有するセッション秘密鍵を計算するセッション鍵生成手段と、

当該ユーザ端末から送信するパケットに対し、改ざんがないことをセッション秘密鍵で保証する処理をするパケット暗号処理手段を備え、

アプリケーションサーバは、

アプリケーションサーバの秘密鍵とユーザ端末の公開鍵とからユーザ端末と共有するセッション秘密鍵を計算するセッション鍵生成手段と、

受信したユーザ端末からのパケットに対し、上記セッション秘密鍵を用いてそのパケットが改ざんされているか否かを確認するパケット検証手段と、

パケットが改ざんされていないことが検証されたパケット内チケットに含まれる鍵情報がユーザ端末の秘密鍵と関連する情報であるか否かを検証し、関連する情報でなければ上記チケットのチケット記憶手段への記憶を阻止するチケット検証手段とを備える。

[3] 請求の範囲2の認証システムにおいて、

上記ユーザ端末からのチケットの送信はパケットにより行われ、

アプリケーションサーバは、

ユーザ端末から送信されたチケット中のアドレスと、そのチケットを含むパケットの送信元アドレスとを照合し、一致しなければ上記チケットの記憶を阻止するアドレス照合

手段を備える。

[4] 請求の範囲2の認証システムにおいて、

認証サーバは上記ユーザの認証に成功するとその認証要求に対し上記認証したユーザと対応するユーザ識別子を割当てるユーザ識別子割当手段を備え、

上記チケット発行手段は上記チケットを、上記ユーザ識別子も含めて発行する手段である。

[5] 請求の範囲1ー4のいずれかの認証システムにおいて、

認証サーバのチケット発行手段は、認証サーバとアプリケーションサーバとの間で事前に共有する共有秘密鍵を用いて仮のチケットについての認証情報を生成する認証情報生成手段を含み、上記認証情報を含むチケットを発行する手段であり、

アプリケーションサーバのチケット検証手段は、

認証サーバとアプリケーションサーバとの間で事前に共有する共有秘密鍵を用いてチケットに含まれる認証情報に対し、改ざんの有無を検証し、改ざんされていれば上記チケットのチケット記憶手段へ記憶を阻止する認証情報検証部を備える。

[6] 請求の範囲1又は4の認証システムにおいて、

上記ユーザ端末からのチケットの送信はパケットにより行われ、

アプリケーションサーバは、

ユーザ端末から送信されたチケット中のアドレスと、そのチケットを含むパケットの送信元アドレスとを照合し、一致しなければ上記チケットの記憶を阻止するアドレス照合手段を備える。

[7] ユーザ端末を介してその利用ユーザに対する認証が認証サーバにより行われ、その認証に基づき、アプリケーションサーバにサービスの提供要求をする認証システムにおける認証サーバであって、

ユーザ端末から送信されたユーザ認証情報を含む認証要求を受信するユーザ認証情報受信手段と、

上記受信された認証要求のユーザ認証情報が入力され、そのユーザ認証情報に基づきそのユーザを認証し、その認証に成功するとこれを示す信号を出力する認証手段と、

上記ユーザの認証に成功したことを示す信号が入力されると上記ユーザ端末にアドレスを割当てるアドレス割当手段と、

上記割当てられたアドレスが入力され、そのアドレスを含むチケットを発行するチケット発行手段と、

上記チケットが入力され、そのチケットを上記ユーザ端末に送信するチケット送信手段と

を備える認証サーバ。

[8] 請求の範囲7の認証サーバにおいて、

認証サーバとアプリケーションサーバとの間に事前に共有する共有秘密鍵を用いて少なくとも上記割当てられたアドレスを含む情報について認証情報を生成する認証情報生成手段を備え、

上記チケット発行手段は上記チケットを上記認証情報も含めて発行する手段である。

[9] 請求の範囲7の認証サーバにおいて、

上記ユーザの認証に成功したことを示す信号が入力されると、上記認証したユーザと対応するユーザ識別子を上記認証要求に割当てるユーザ識別子割当手段を備え、

上記チケット発行手段は上記チケットを、上記ユーザ識別子も含めて発行する手段である。

[10] 請求の範囲9の認証サーバにおいて、

上記ユーザ識別子割当手段は上記ユーザを直接識別する情報が入力され、当該認証サーバの識別子生成用秘密鍵により上記ユーザを直接識別する情報を暗号化し、その暗号化情報を上記ユーザ識別子とする手段である。

[11] 請求の範囲7ー10のいずれかの認証サーバにおいて、

上記ユーザ端末の秘密鍵と関連した鍵情報が上記認証要求に含まれ、

上記チケット発行手段は、上記チケットを上記鍵情報も含めて発行する手段である。

[12] ユーザ端末を介してその利用ユーザに対する認証が認証サーバにより行われ、そ

の認証に基づき、アプリケーションサーバにサービスの提供要求をする認証システムにおけるユーザ端末であって、

入力されたユーザ認証情報を認証サーバへ送信して認証要求をするユーザ認証情報送信手段と、

認証サーバから送信されたチケットを受信するチケット受信手段と、

受信したチケットが入力され、チケットに含まれるアドレスを当該ユーザ端末の送信元アドレスとして設定する送信元アドレス設定手段と、

上記チケットが入力され、そのチケットを含むパケットをアプリケーションサーバへ送信して、そのアプリケーションサーバとの間にセッションを確立するセッション確立手段と

上記確立されたセッションを通して、サービスの要求を表わすパケットを上記アプリケーションサーバへ送信するサービス要求手段と

を備えるユーザ端末。

[13] 請求の範囲12のユーザ端末において、

当該ユーザ端末の公開鍵が入力され、その公開鍵と関連した鍵情報を生成する鍵情報生成手段と、

当該ユーザ端末の秘密鍵と上記アプリケーションサーバの公開鍵とが入力され、これらから上記アプリケーションサーバと共有するセッション秘密鍵を計算するセッション鍵生成手段と、

当該ユーザ端末から送信するパケット及び上記セッション秘密鍵が入力され、その送信するパケットに対し、改ざんがないことを上記セッション秘密鍵で保証する処理をするパケット暗号処理手段とを備え、

上記ユーザ認証情報送信手段は上記鍵情報も入力され、その鍵情報を上記ユーザ認証情報と共に送信して上記認証要求をする手段である。

[14] 請求の範囲12のユーザ端末において、

上記アプリケーションサーバと共有の認証用共有秘密鍵と上記セッション確立ごとに変化するセッション依存情報とが入力され、上記認証用共有秘密鍵により上記セッション依存情報を処理して鍵情報を生成する鍵情報生成手段を備え、

上記ユーザ認証情報送信手段は上記鍵情報も入力され、その鍵情報を上記ユーザ認証情報と共に送信して上記認証要求をする手段である。

[15] ユーザ端末を介してその利用ユーザに対する認証が認証サーバにより行われ、その認証に基づき、アプリケーションサーバにサービスの提供要求をする認証システムにおけるアプリケーションサーバであって、

ユーザ端末とセッションを確立するセッション確立手段と、

ユーザ端末から送信されたチケットが記憶されるチケット記憶手段と、

上記確立されたセッションを通じてユーザ端末から送信され、受信したサービス要求パケットの送信元アドレスが入力され、その送信元アドレスとチケット記憶手段に記憶されているチケットに含まれるアドレスとが一致するか否かを判断するアドレス判断手段と、

アドレス判断手段からの一致と判断された出力が入力され、ユーザにサービスを提供するためのパケットを上記ユーザ端末へ送信するサービス提供手段と

を備えるアプリケーションサーバ。

[16] 請求の範囲15のアプリケーションサーバにおいて、

上記受信したパケット中のチケットが入力され、そのチケットの正当性を検証し、正当性がないと検証した出力により上記チケットの記憶を阻止するチケット検証手段を備える。

[17] 請求の範囲16のアプリケーションサーバにおいて、

アプリケーションサーバの秘密鍵とユーザ端末の公開鍵とからユーザ端末と共有するセッション秘密鍵を計算するセッション鍵生成手段と、

受信したユーザ端末からのパケットに対し、上記セッション秘密鍵を用いてそのパケットが改ざんされているか否かを検証し、改ざんされたと検証した出力により上記チケットの記憶を阻止するパケット検証手段を備える。

[18] 請求の範囲17のアプリケーションサーバにおいて、

上記チケット検証手段はパケット検証手段よりの改ざんされていないと検証したパケットが入力され、そのパケット内のチケットに含まれる、上記ユーザ端末の公開鍵と関連する鍵情報と、上記セッション秘密鍵の計算に用いたユーザ端末の公開鍵とが対

応するか否かを検証する手段である。

[19] 請求の範囲16のアプリケーションサーバにおいて、

上記チケット検証手段は上記ユーザ端末と共有の認証用共有秘密鍵と上記セッション確立ごとに変化するセッション依存情報が入力され、その認証用共有秘密鍵により上記セッション依存情報を処理し、その処理結果と上記チケット内の鍵情報とを照合し、その整合性がとれるか否かにより上記チケットの正当性を検証する手段である。

[20] 請求の範囲16，18，19のいずれかのアプリケーションサーバにおいて、

上記チケット検証手段は、上記受信したパケットの送信元アドレスと、そのパケット内のチケットに含まれるアドレスとが一致するか否かを検証し、一致しないと検証した出力により上記チケットの記憶を阻止する手段を含む。

[21] 請求の範囲7ー11のいずれかの認証サーバとしてコンピュータを機能させるための認証サーバプログラム。

[22] 請求の範囲12ー14のいずれかのユーザ端末としてコンピュータを機能させるためのユーザ端末プログラム。

[23] 請求の範囲15ー20のいずれかのアプリケーションサーバとしてコンピュータを機能させるためのアプリケーションサーバプログラム。

[図1]

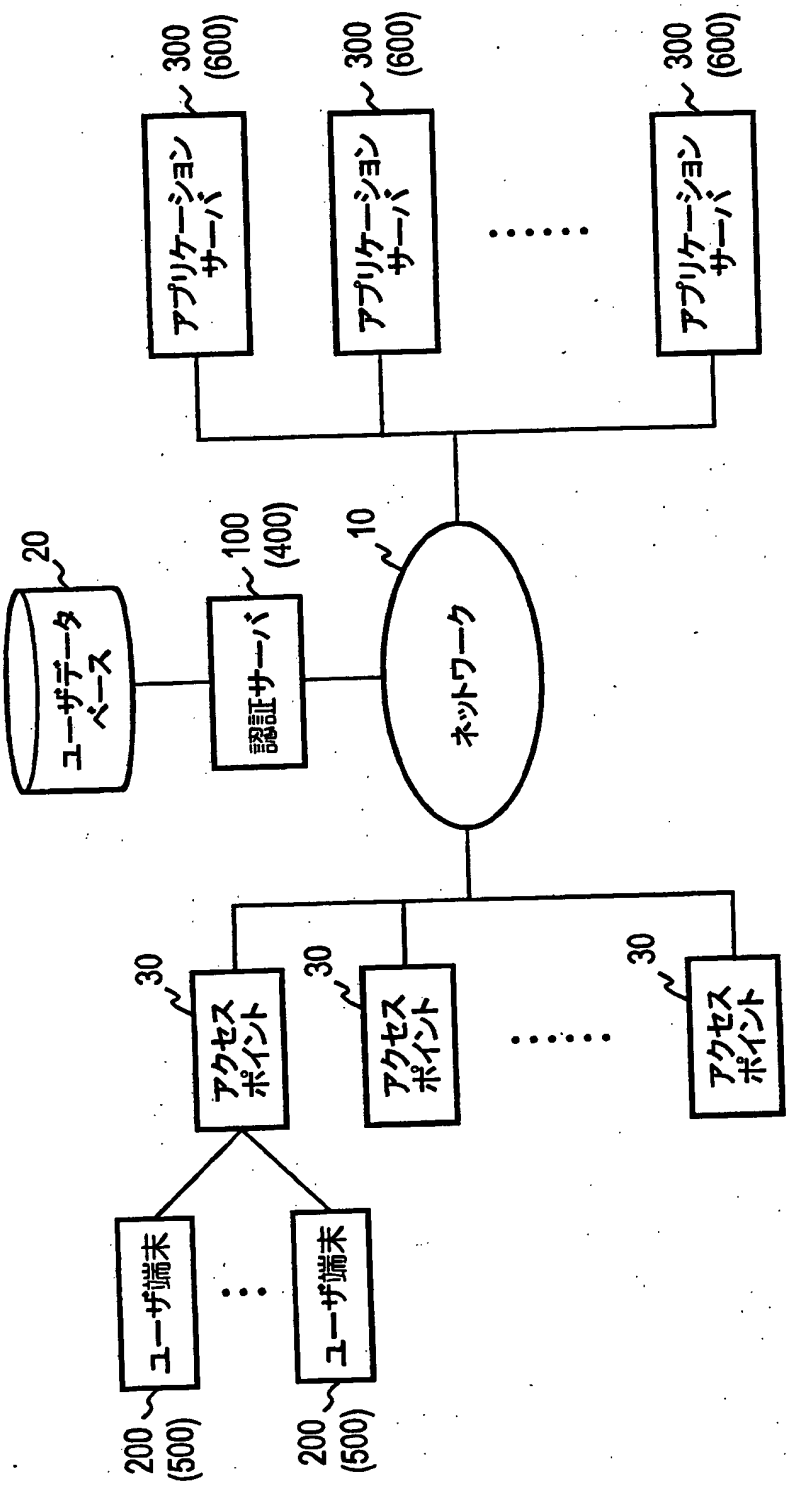

300
(600)
アプリケーション
サーバ
300
(600)
アプリケーション
サーバ
300
(600)
アプリケーション
サーバ
20
ユーザデータ
ベース
100
(400)
認証サーバ
10
ネットワーク
30
アクセス
ポイント
30
アクセス
ポイント
30
アクセス
ポイント
200
(500)
ユーザ端末
200
(500)
ユーザ端末

図1

[図2]

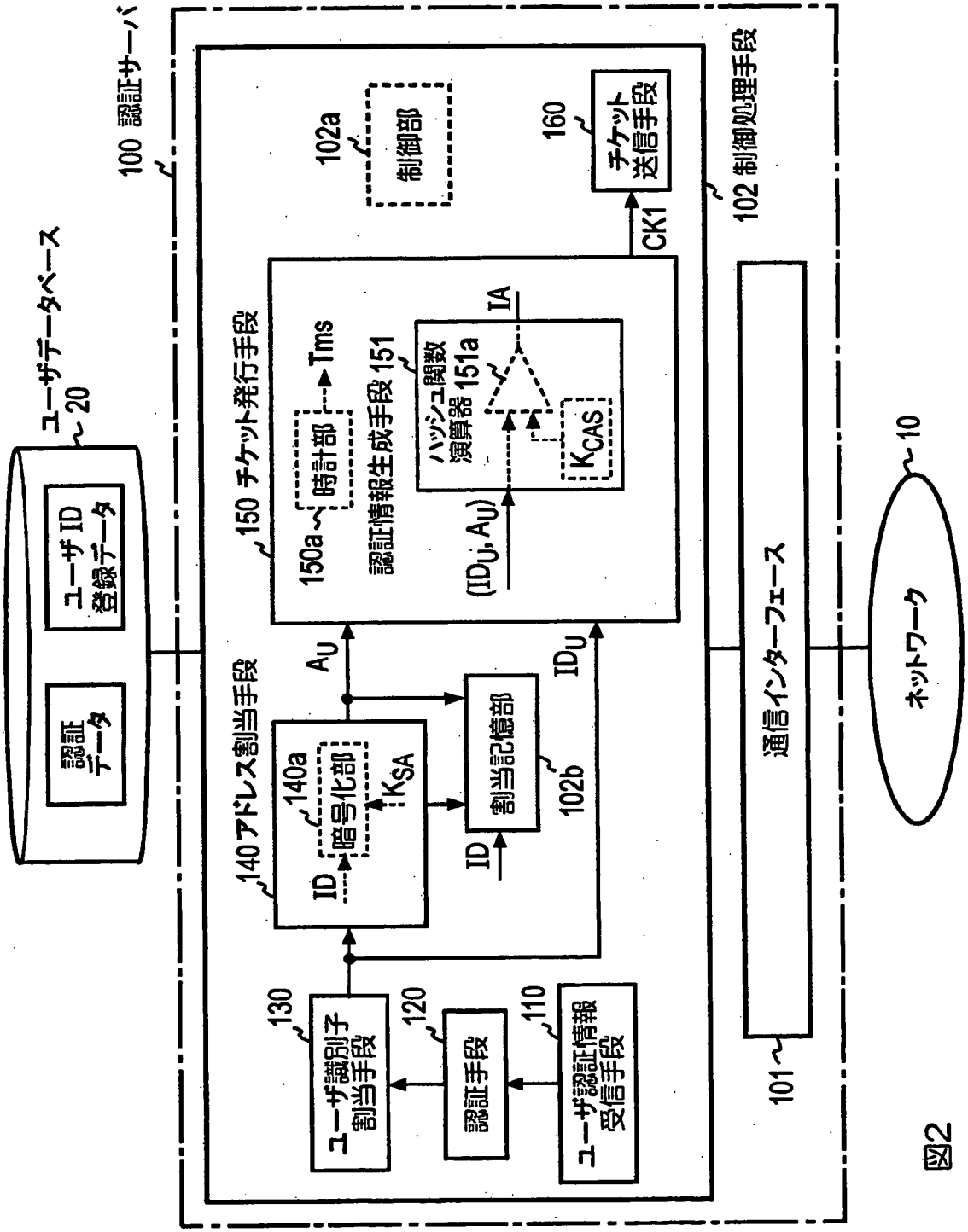

100 認証サーバ
ユーザデータベース 20
認証データ
ユーザID登録データ
102 制御処理手段
102a 制御部
160 チケット送信手段
CK1
150 チケット発行手段
150a 時計部
Tms
認証情報生成手段 151
ハッシュ関数演算器 151a
IA
K_{CAS}
(ID_U, A_U)
A_U
ID_U
140 アドレス割当手段
140a
ID
暗号化部
K_{SA}
割当記憶部
102b
ID
130 ユーザ識別子割当手段
120 認証手段
110 ユーザ認証情報受信手段
101
通信インターフェース
ネットワーク 10

図2

[図3]

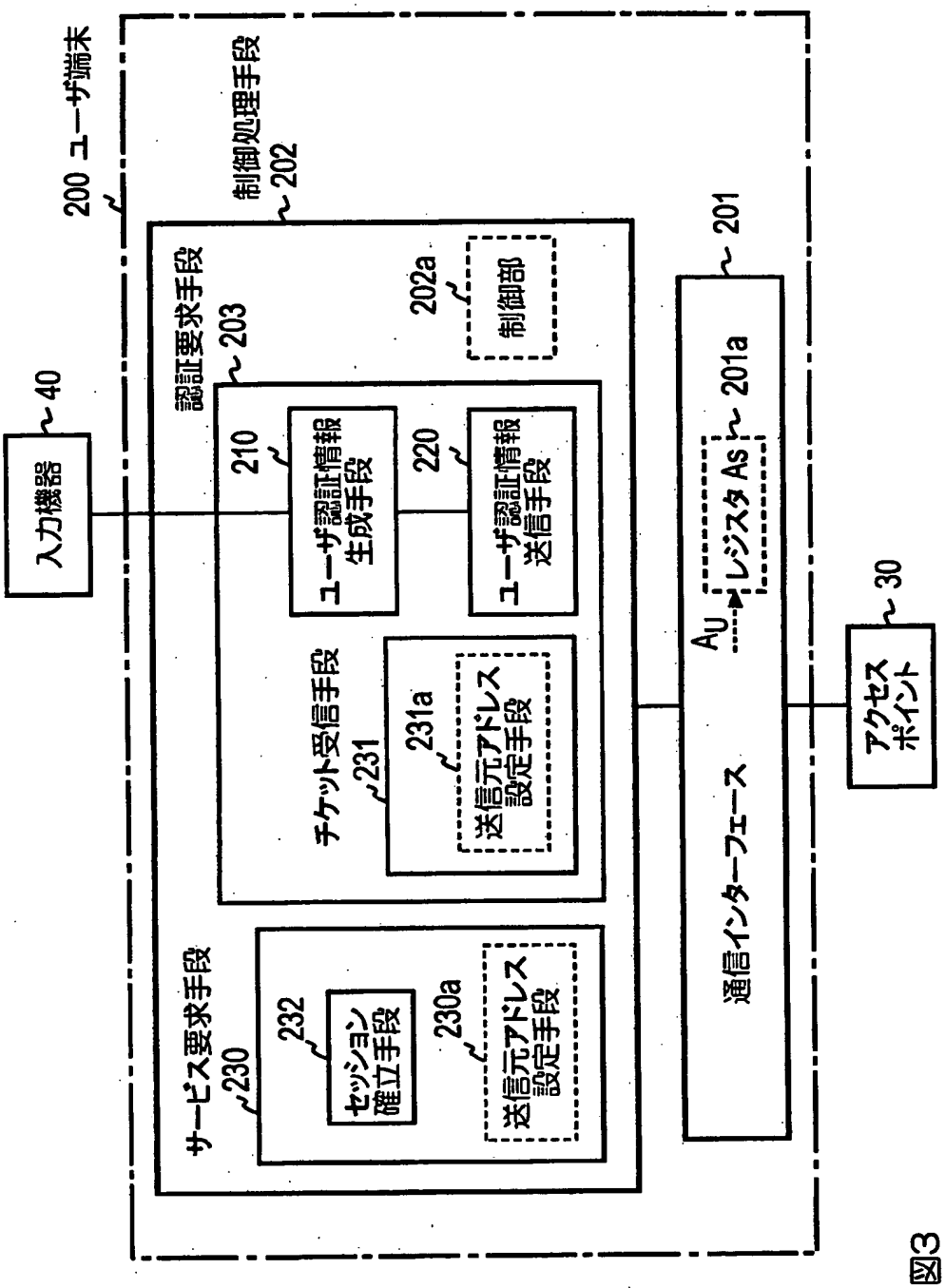

200 ユーザ端末
制御処理手段
202
認証要求手段
203
202a
制御部
40
入力機器
210
ユーザ認証情報
生成手段
220
ユーザ認証情報
送信手段
201
201a
レジスタ As
AU
チケット受信手段
231
231a
送信元アドレス
設定手段
30
アクセス
ポイント
サービス要求手段
230
232
セッション
確立手段
230a
送信元アドレス
設定手段
通信インターフェース

図3

[図4]

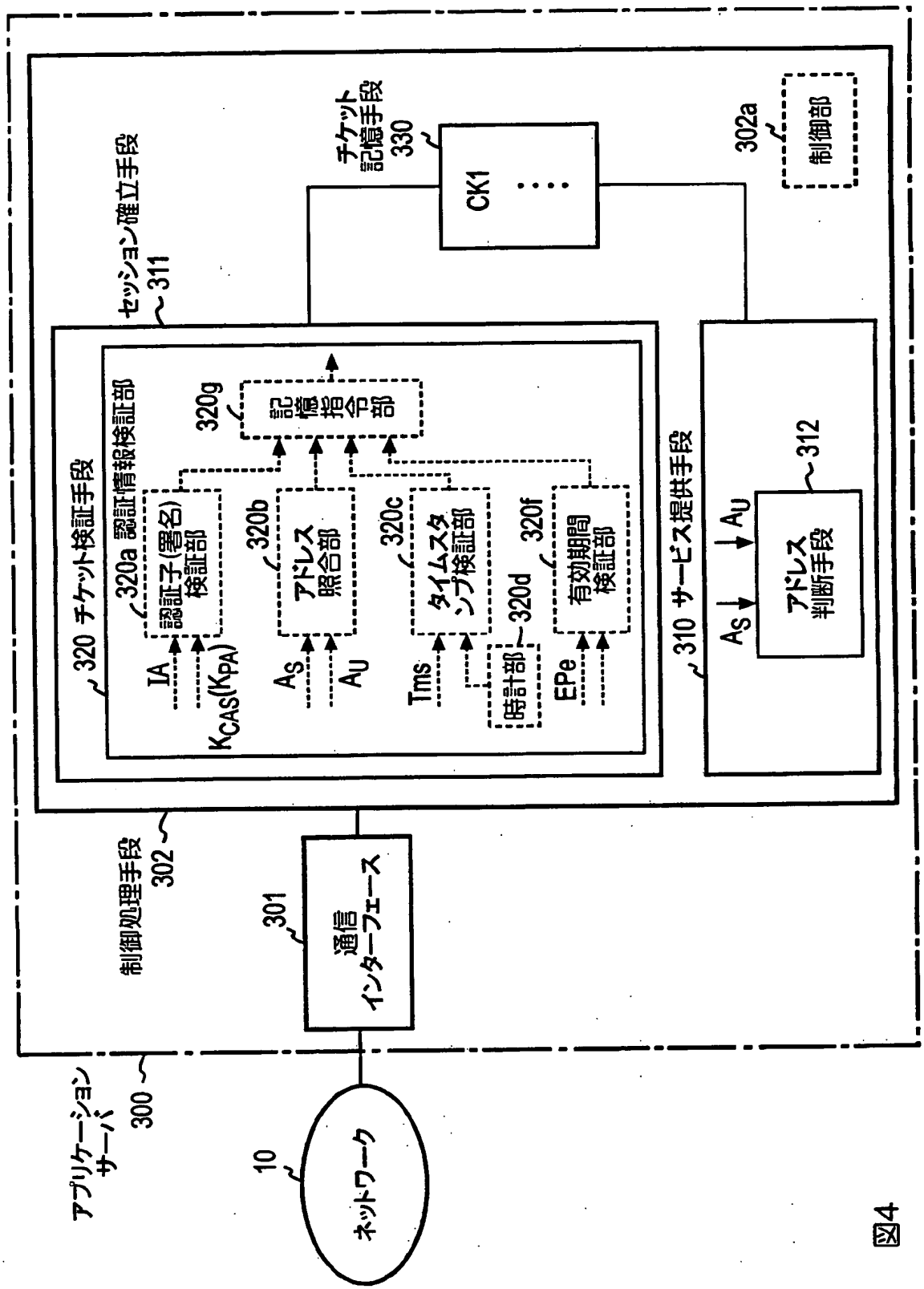

アプリケーションサーバ
300
ネットワーク
10
制御処理手段
302
通信インターフェース
301
セッション確立手段
311
チケット検証手段
320
認証情報検証部
320a
認証子(署名)検証部
IA
$K_{CAS}(K_{PA})$
アドレス照合部
320b
A_S
A_U
タイムスタンプ検証部
320c
Tms
時計部
320d
有効期間検証部
320f
EPe
記憶指令部
320g
チケット記憶手段
330
CK1
サービス提供手段
310
アドレス判断手段
312
制御部
302a

図4

[図5]

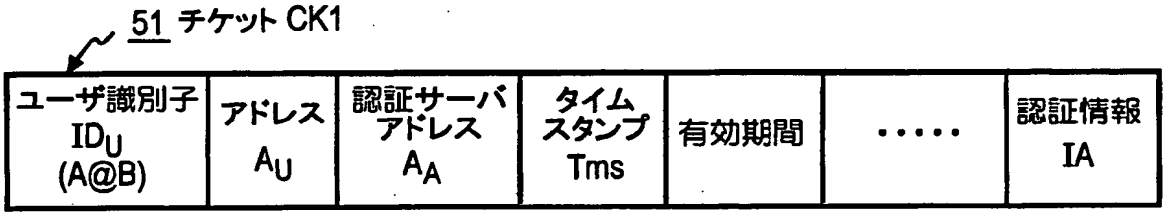

51 チケット CK1
ユーザ識別子 ID_U (A@B)
アドレス A_U
認証サーバアドレス A_A
タイムスタンプ Tms
有効期間
.....
認証情報 IA

図5

[図6]

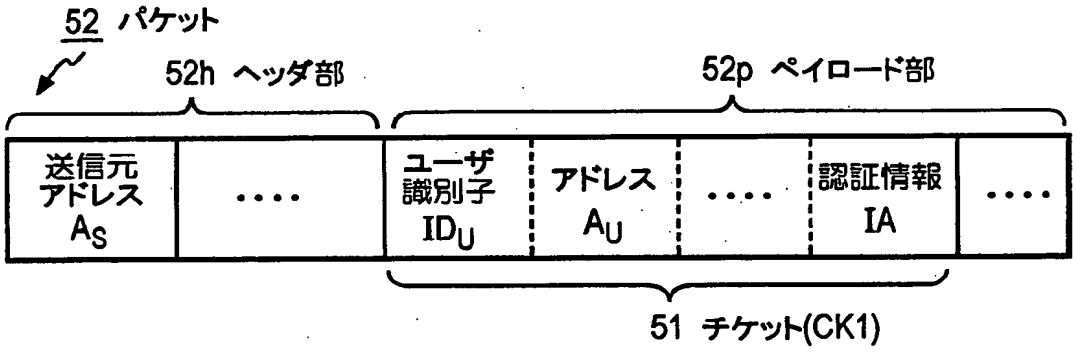

52 パケット
52h ヘッダ部
52p ペイロード部
送信元アドレス A_S
....
ユーザ識別子 ID_U
アドレス A_U
....
認証情報 IA
....
51 チケット(CK1)

図6

[図7]

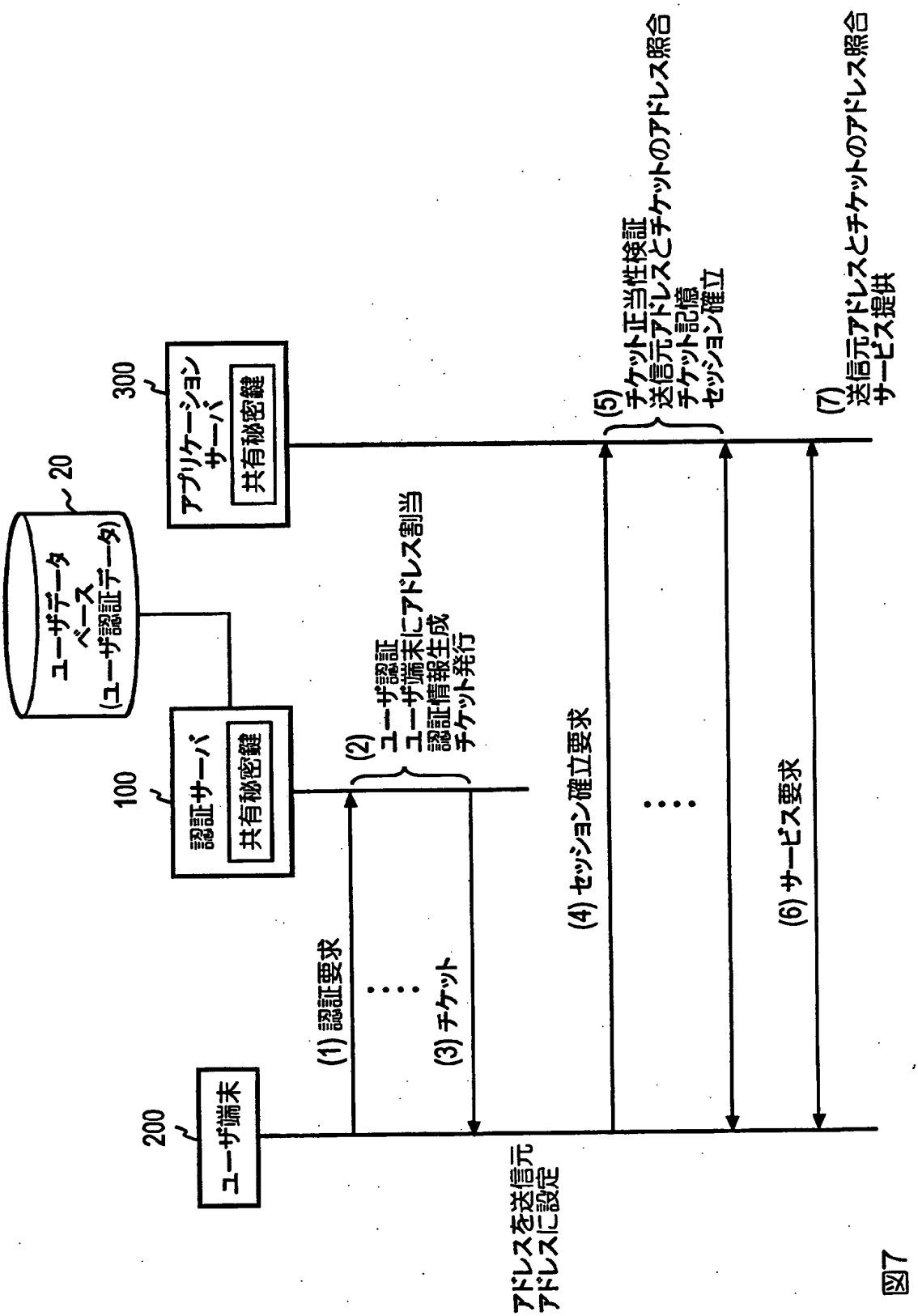

ユーザ端末
200
認証サーバ
共有秘密鍵
100
ユーザデータベース
(ユーザ認証データ)
20
アプリケーションサーバ
共有秘密鍵
300
(1) 認証要求
(2) ユーザ認証
ユーザ端末にアドレス割当
認証情報生成
チケット発行
(3) チケット
(4) セッション確立要求
(5) チケット正当性検証
送信元アドレスとチケットのアドレス照合
チケット記憶
セッション確立
(6) サービス要求
(7) 送信元アドレスとチケットのアドレス照合
サービス提供
アドレスを送信元
アドレスに設定

図7

[図8]

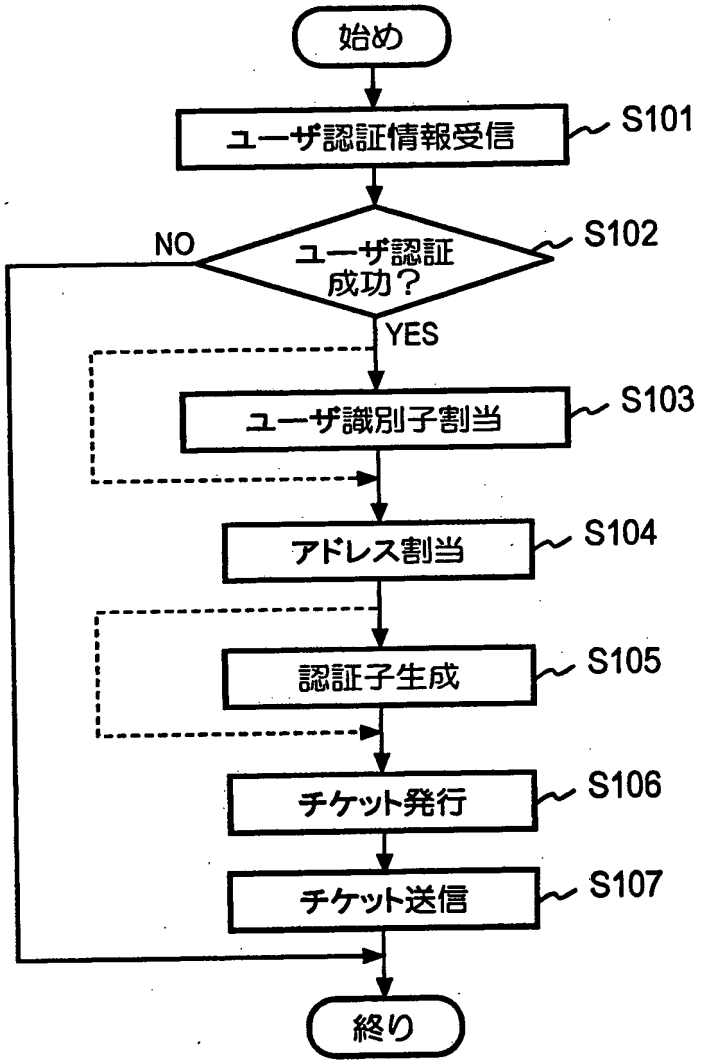

始め
ユーザ認証情報受信
S101
NO
ユーザ認証成功？
S102
YES
ユーザ識別子割当
S103
アドレス割当
S104
認証子生成
S105
チケット発行
S106
チケット送信
S107
終り

図8

[図9]

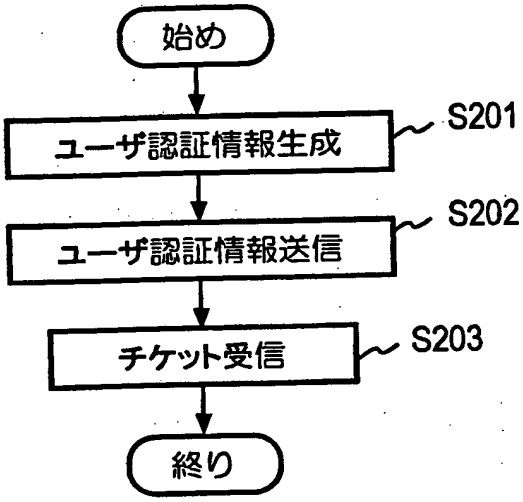

始め
ユーザ認証情報生成
S201
ユーザ認証情報送信
S202
チケット受信
S203
終り

図9A

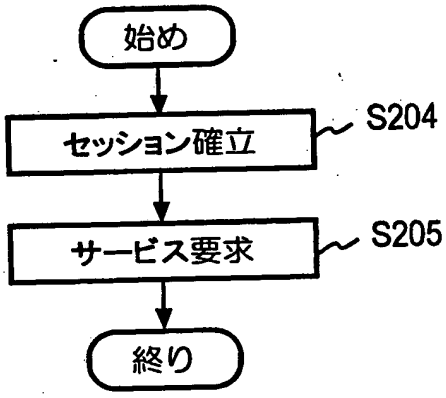

始め
セッション確立
S204
サービス要求
S205
終り

図9B

[図10]

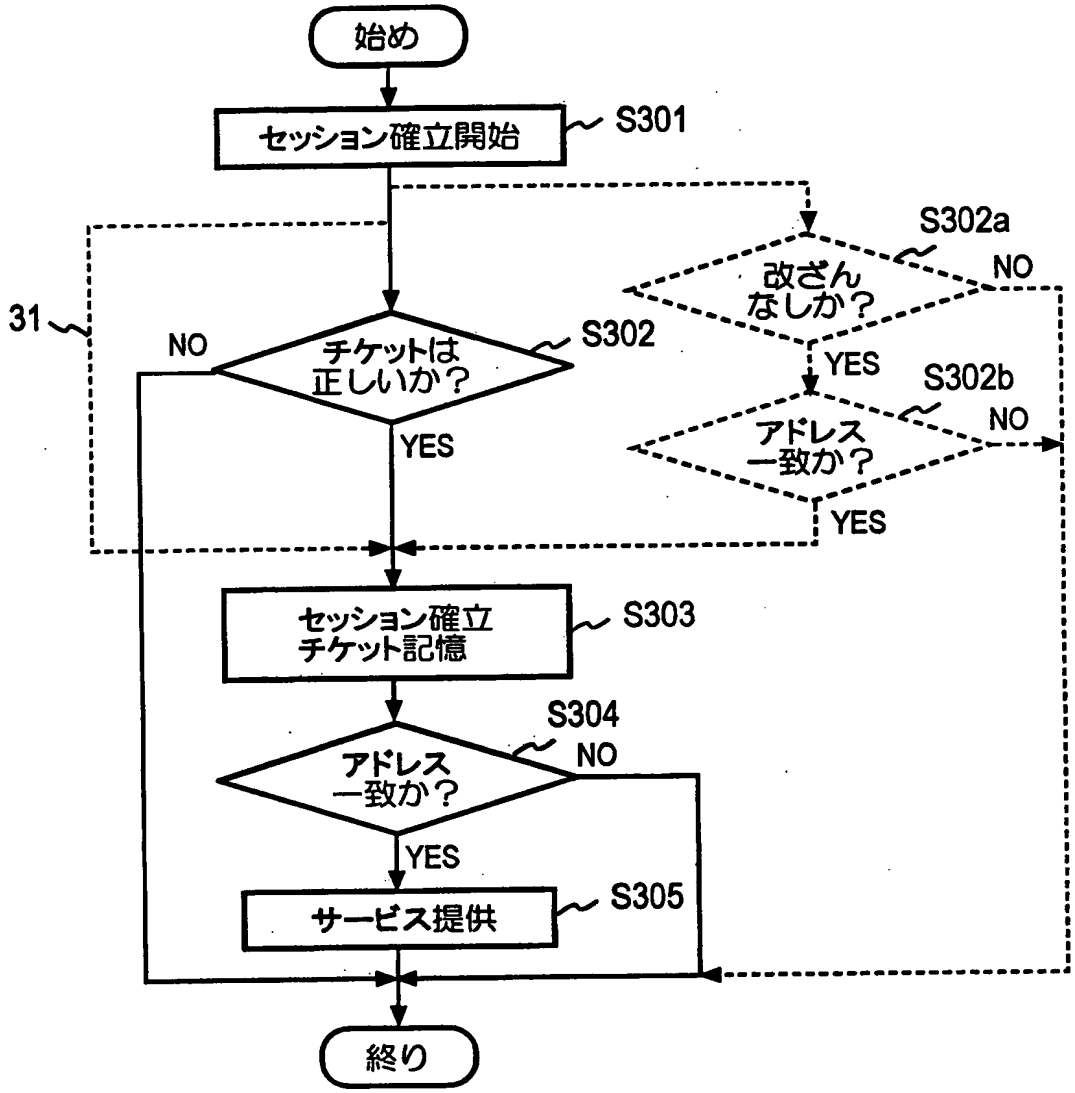

始め
セッション確立開始
S301
S302a
改ざん
なしか？
NO
YES
31
NO
チケットは
正しいか？
S302
YES
S302b
アドレス
一致か？
NO
YES
セッション確立
チケット記憶
S303
S304
アドレス
一致か？
NO
YES
サービス提供
S305
終り

図10

[図11]

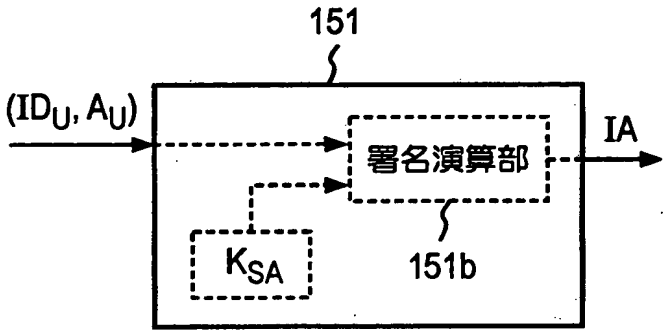


図11A

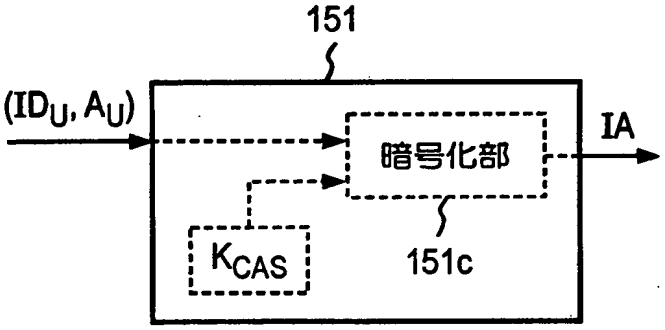


図11B

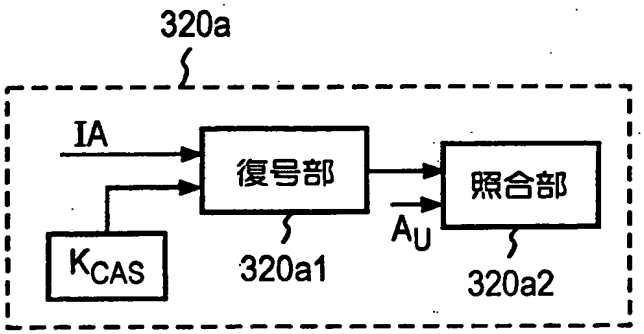


図11C

[図12]

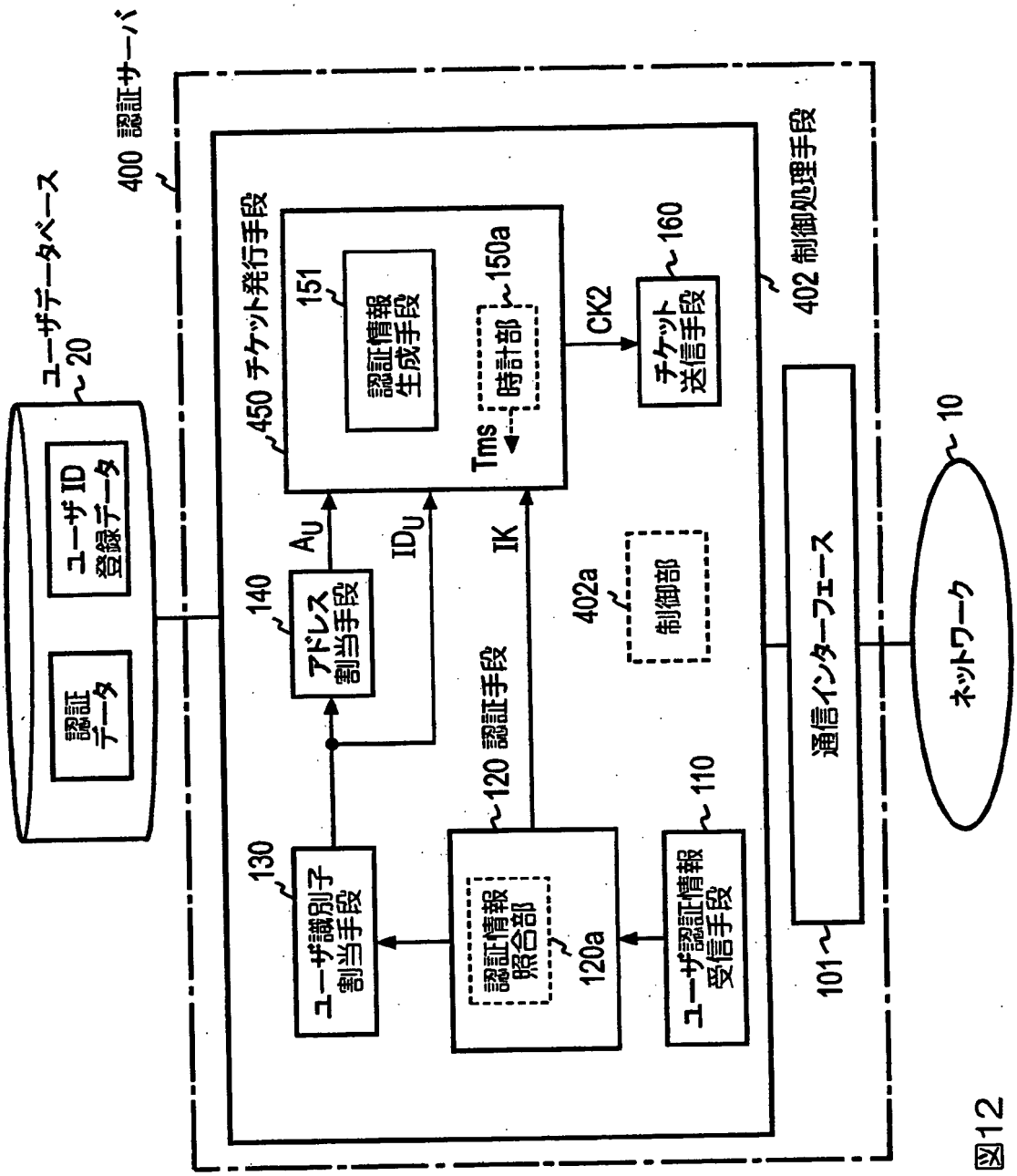

400 認証サーバ
ユーザデータベース
20
ユーザ ID 登録データ
認証データ
450 チケット発行手段
151
認証情報生成手段
150a
時計部
Tms
CK2
160
チケット送信手段
402 制御処理手段
140
アドレス割当手段
A_U
ID_U
IK
402a
制御部
120 認証手段
130
ユーザ識別子割当手段
認証情報照合部
120a
110
ユーザ認証情報受信手段
通信インターフェース
101
10
ネットワーク

図12

[図13]

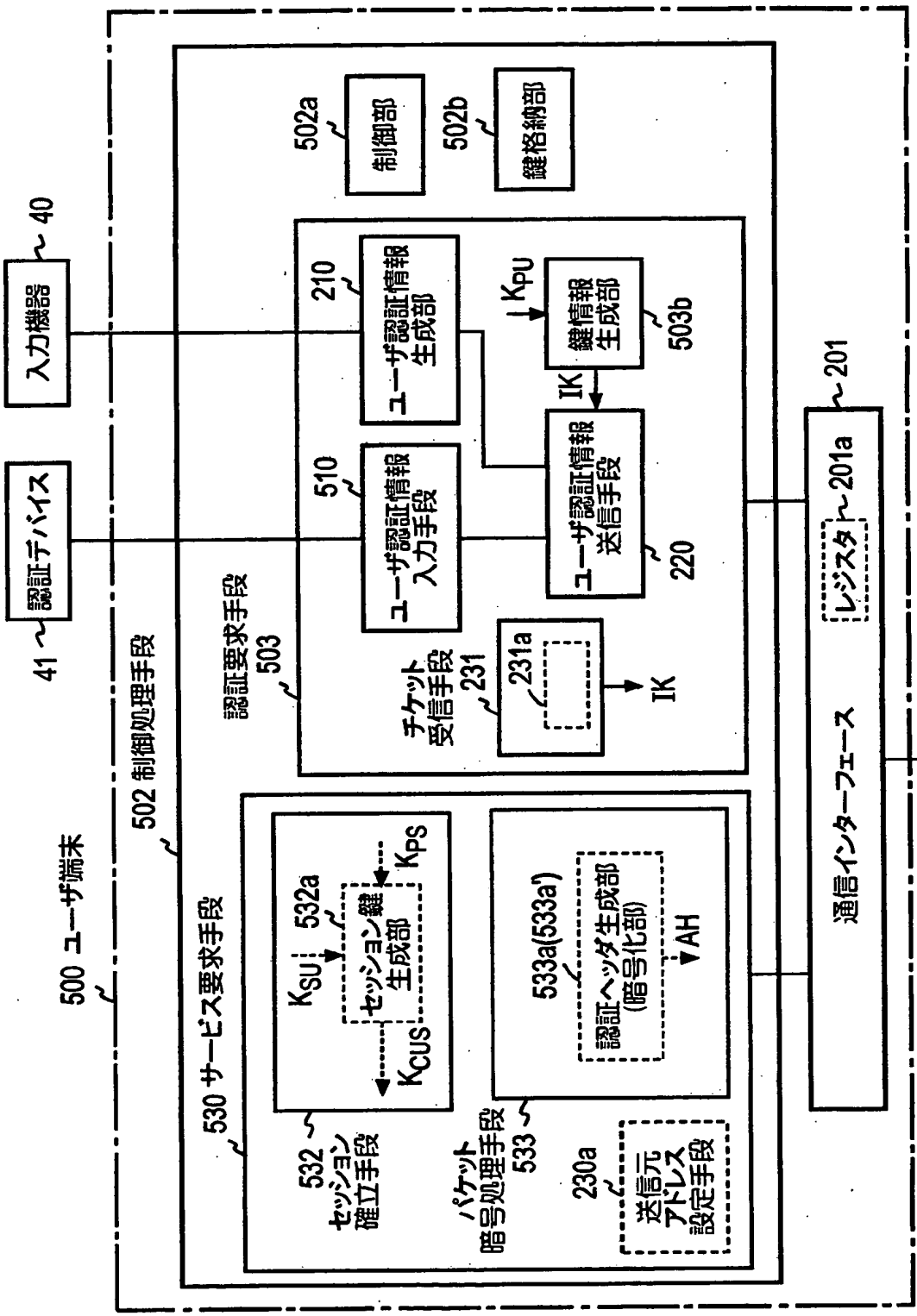

500 ユーザ端末
502 制御処理手段
530 サービス要求手段
532 セッション確立手段
K_{SU}
532a
セッション鍵 生成部
K_{PS}
K_{CUS}
パケット暗号処理手段 533
533a(533a')
認証ヘッダ生成部 (暗号化部)
AH
230a
送信元アドレス設定手段
認証要求手段 503
チケット受信手段 231
231a
IK
ユーザ認証情報入力手段 510
ユーザ認証情報送信手段 220
ユーザ認証情報生成部 210
K_{PU}
鍵情報生成部 503b
IK
制御部 502a
鍵格納部 502b
入力機器 40
認証デバイス 41
通信インターフェース
レジスタ 201a
201
アクセスポイント 30

図13

[図14]

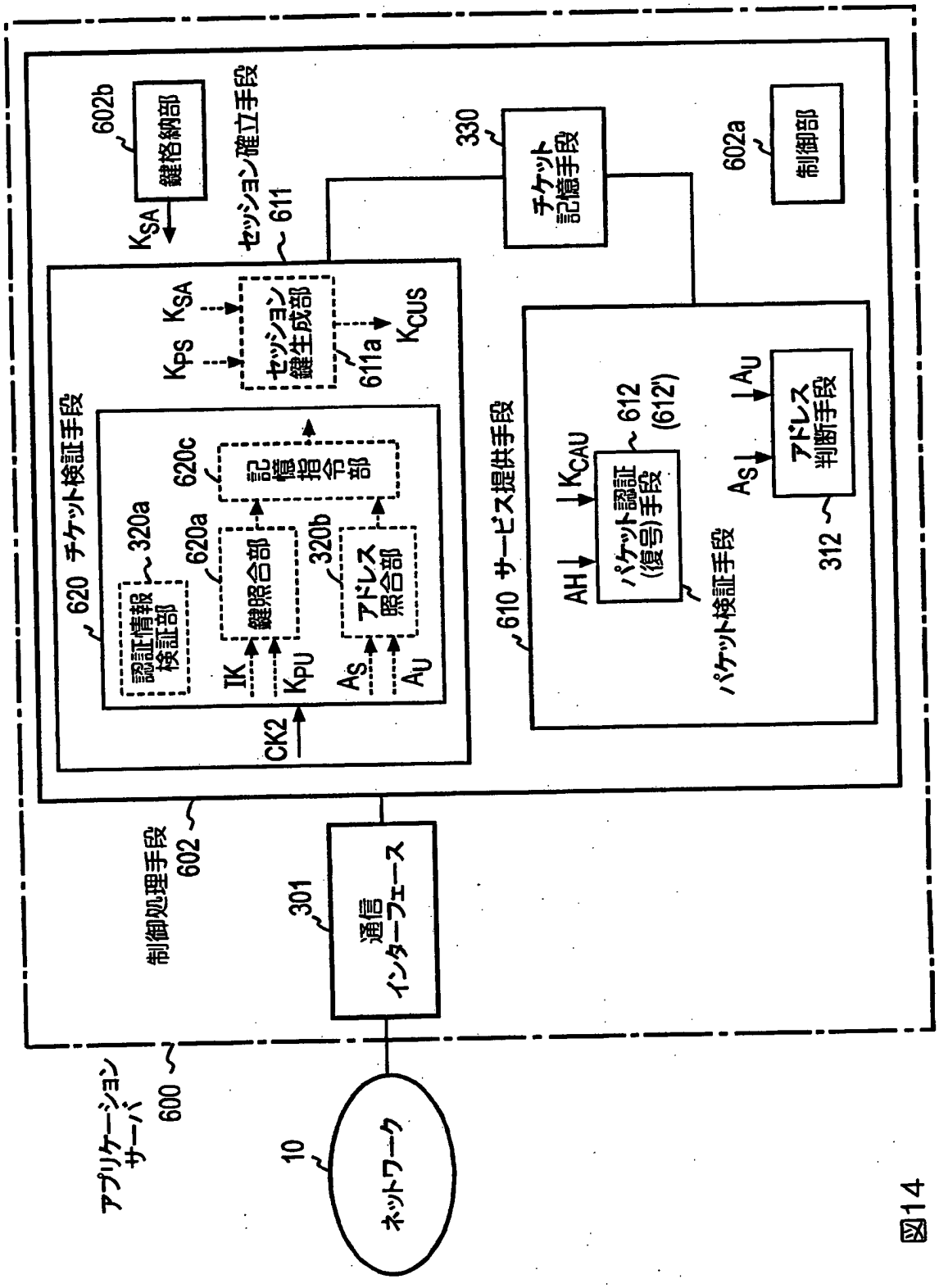

アプリケーションサーバ
600
ネットワーク
10
通信インターフェース
301
制御処理手段
602
チケット検証手段
620
認証情報検証部
320a
鍵照合部
620a
アドレス照合部
320b
記憶指令部
620c
セッション鍵生成部
611a
セッション確立手段
611
鍵格納部
602b
サービス提供手段
610
パケット検証手段
パケット認証(復号)手段
612
(612')
アドレス判断手段
312
チケット記憶手段
330
制御部
602a
IK
KPU
AS
AU
CK2
KSA
KPS
KCUS
AH
KCAU

図14

[図15]

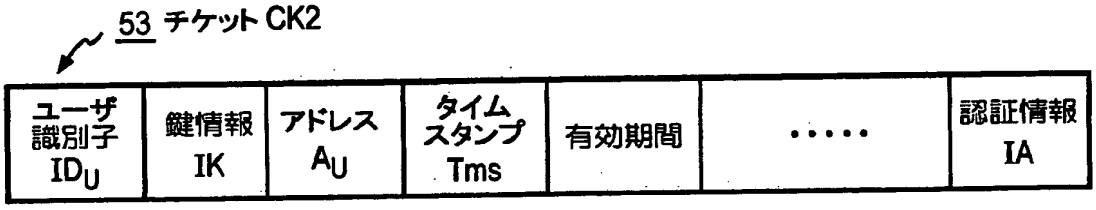


図15

[図16]

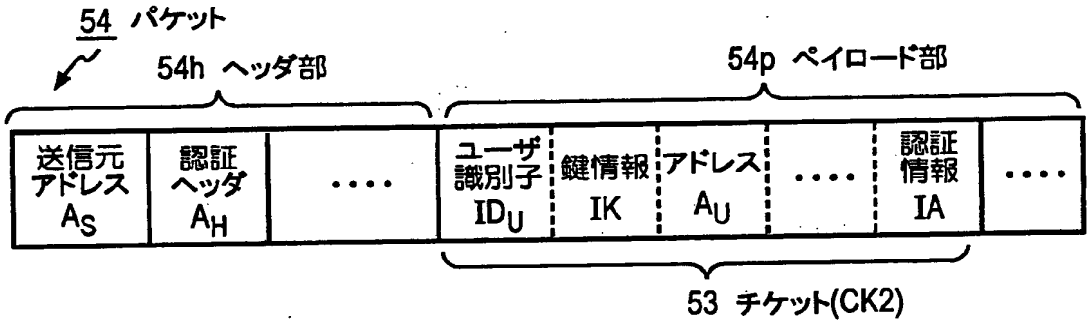


図16

[図17]

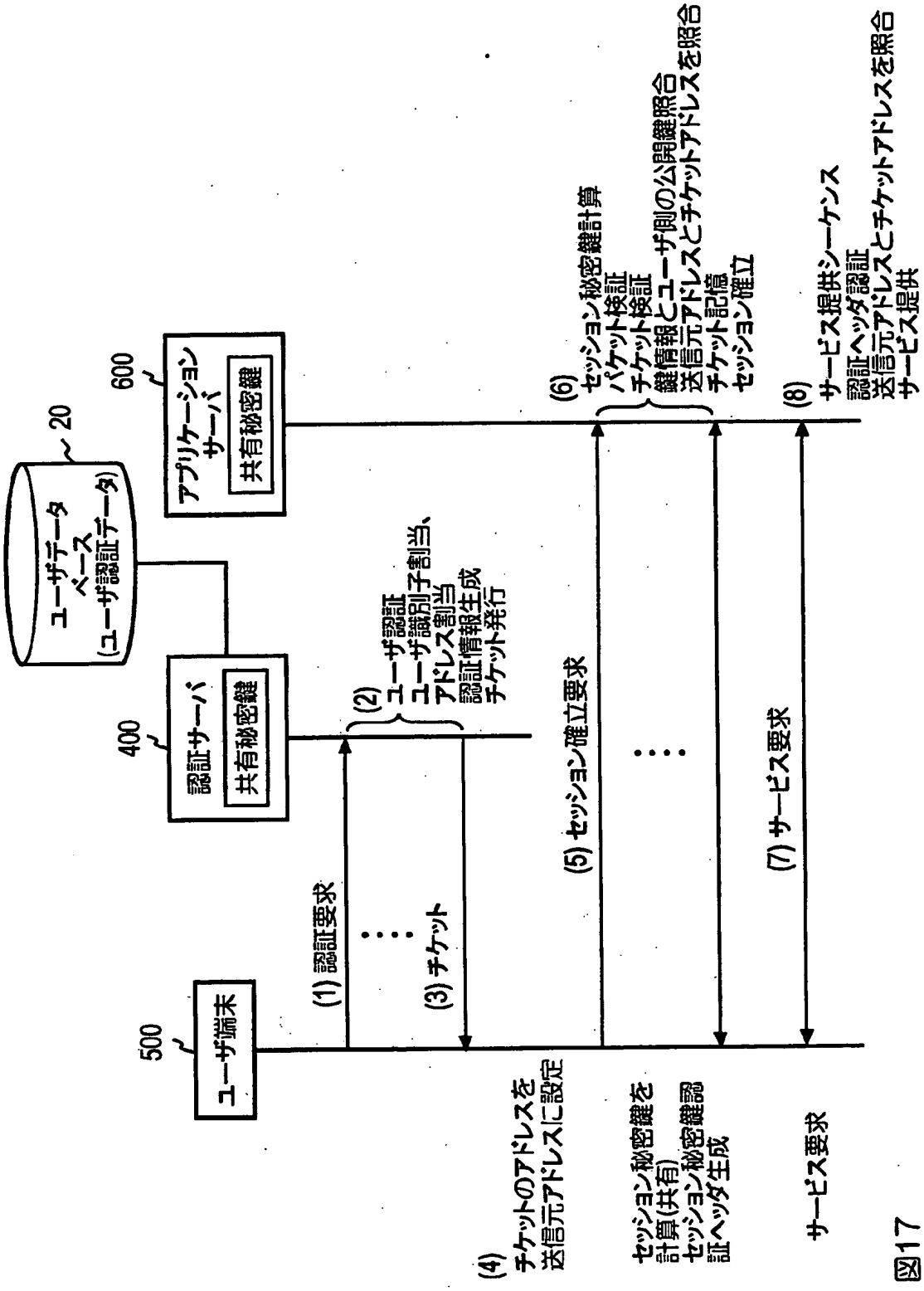

ユーザ端末
500
認証サーバ
共有秘密鍵
400
ユーザデータベース
(ユーザ認証データ)
20
アプリケーションサーバ
共有秘密鍵
600
(1) 認証要求
(2) ユーザ認証
ユーザ識別子割当、
アドレス割当
認証情報生成
チケット発行
(3) チケット
(4) チケットのアドレスを送信元アドレスに設定
(5) セッション確立要求
(6) セッション秘密鍵計算
パケット検証
チケット検証
鍵情報とユーザ側の公開鍵照合
送信元アドレスとチケットアドレスを照合
チケット記憶
セッション確立
セッション秘密鍵を計算(共有)
セッション秘密鍵認証ヘッダ生成
(7) サービス要求
サービス要求
(8) サービス提供シーケンス
認証ヘッダ認証
送信元アドレスとチケットアドレスを照合
サービス提供

図17

[図18]

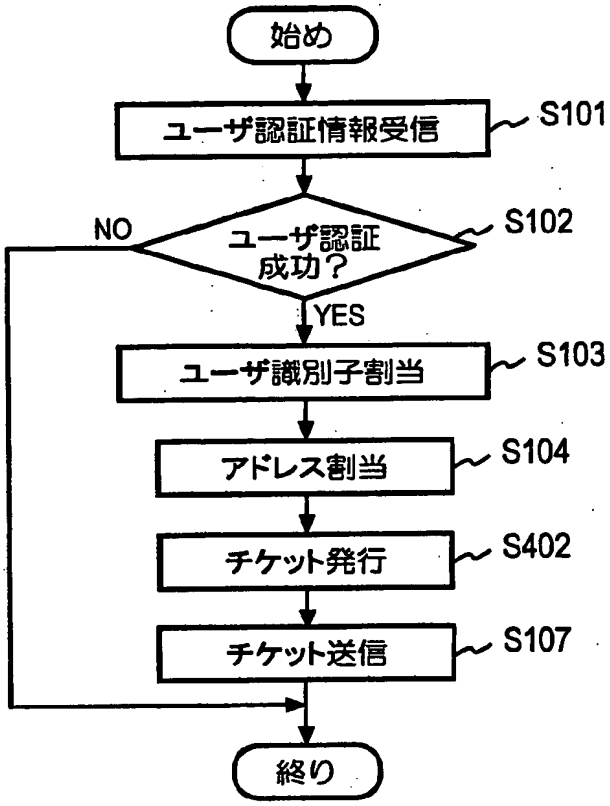


図18

[図19]

図19A

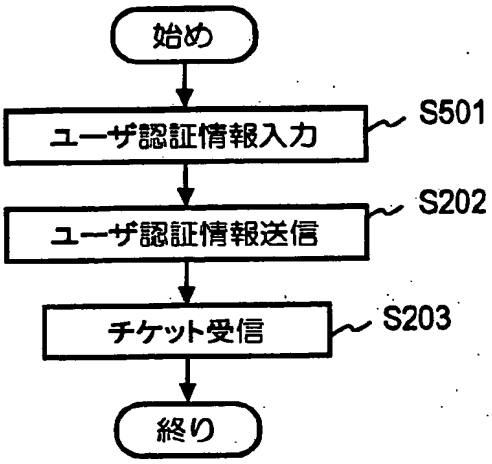
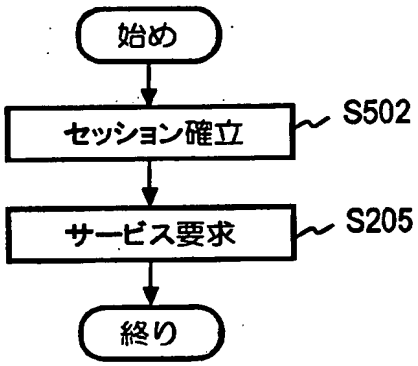


図19B



[図20]

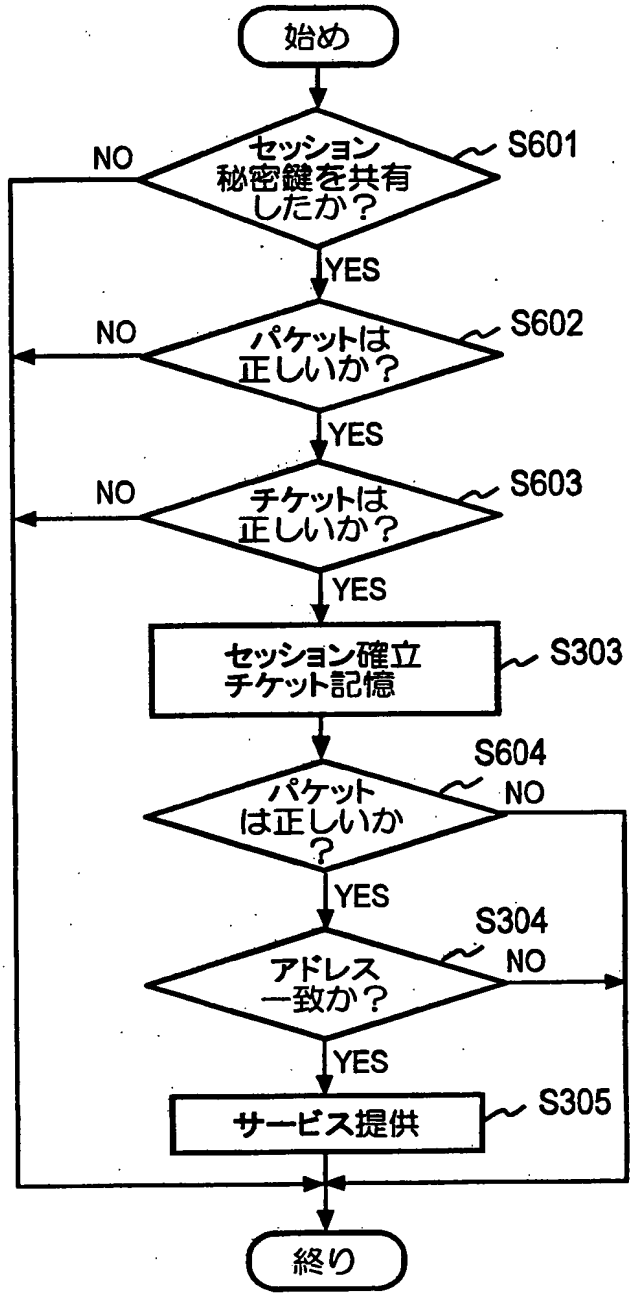

始め
セッション秘密鍵を共有したか？
S601
NO
YES
パケットは正しいか？
S602
NO
YES
チケットは正しいか？
S603
NO
YES
セッション確立チケット記憶
S303
パケットは正しいか？
S604
NO
YES
アドレス一致か？
S304
NO
YES
サービス提供
S305
終り

図20

[図21]

図21A

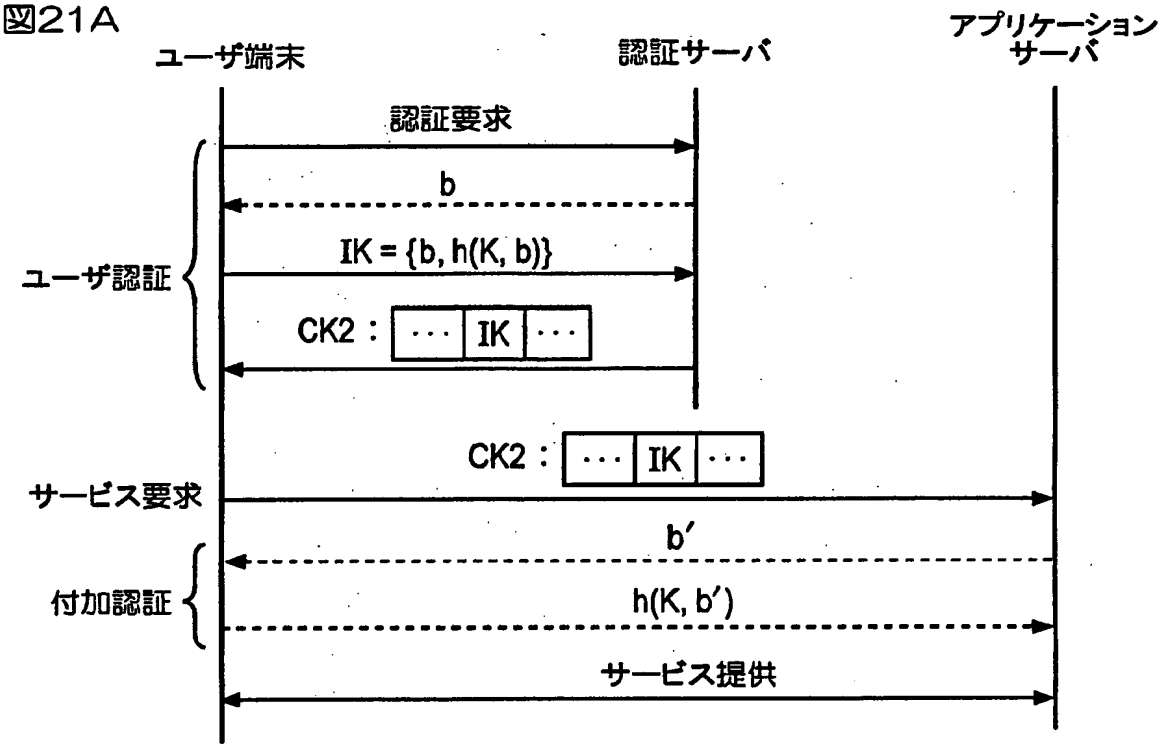


図21B

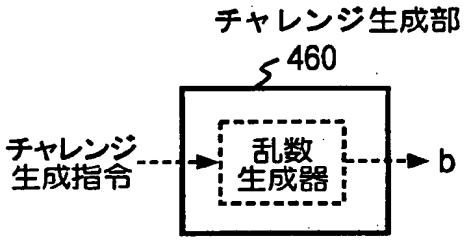


図21C

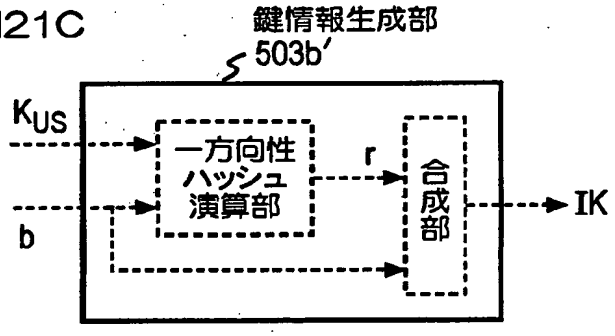
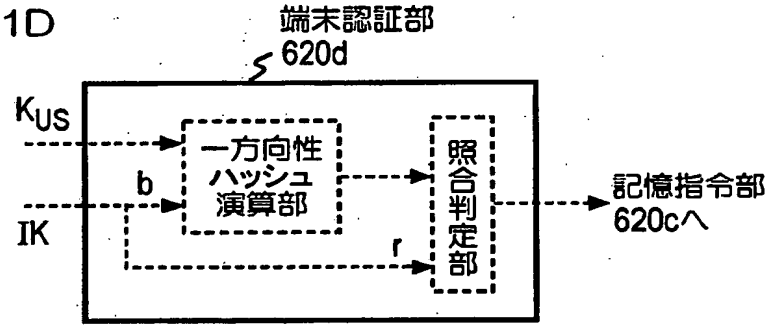


図21D



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009944

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 5-333775 A (Toshiba Corp.), 17 December, 1993 (17.12.93), Full text; Figs. 1 to 6 (Family: none)	1-23
Y	JP 2003-66836 A (Hitachi, Ltd.), 05 March, 2003 (05.03.03), Column 5, lines 35 to 39; Par. Nos. [0014] to [0024], [0026] to [0029], [0034] to [0045], [0047] to [0053], [0063]; Figs. 1 to 4, 6 to 9, 11 (Family: none)	1-23

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 October, 2004 (05.10.04)	09 November, 2004 (09.11.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009944

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 9-330284 A (Hitachi, Ltd.), 22 December, 1997 (22.12.97), Par. Nos. [0011] to [0013]; Figs. 1 to 3 (Family: none)	1-23

国際調査報告

国際出願番号　PCT／JP2004／009944

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／32, H04L9／08

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／32, H04L9／08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　5－333775　A（株式会社東芝） 1993．12．17　全文，図1－6 （ファミリーなし）	1－23
Y	JP　2003－66836　A（株式会社日立製作所） 2003．03．05 第5欄第35－39行，第【0014】－【0024】段落， 第【0026】－【0029】段落， 第【0034】－【0045】段落， 第【0047】－【0053】段落，第【0063】段落，	1－23

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 05．10．2004	国際調査報告の発送日 09.11.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 青木　重徳　5M　4229 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（2004年1月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	図１－４，６－９，１１ （ファミリーなし）	
Ｙ	ＪＰ　９－３３０２８４　Ａ（株式会社日立製作所） １９９７．１２．２２ 第【００１１】－【００１３】段落，図１－３ （ファミリーなし）	１－２３